経済産業省

資料３

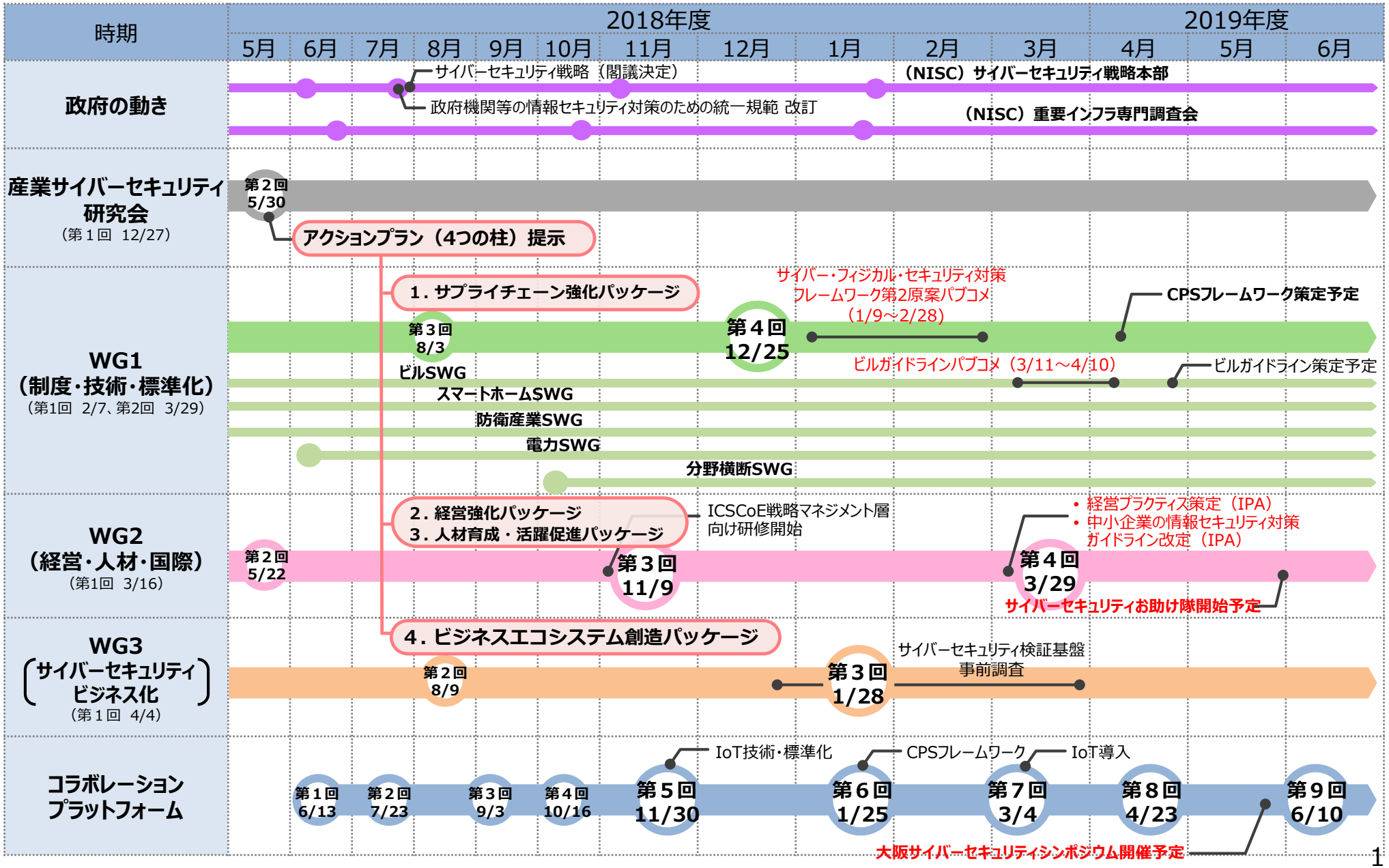
事務局説明資料

経済産業省

商務情報政策局

サイバーセキュリティ課

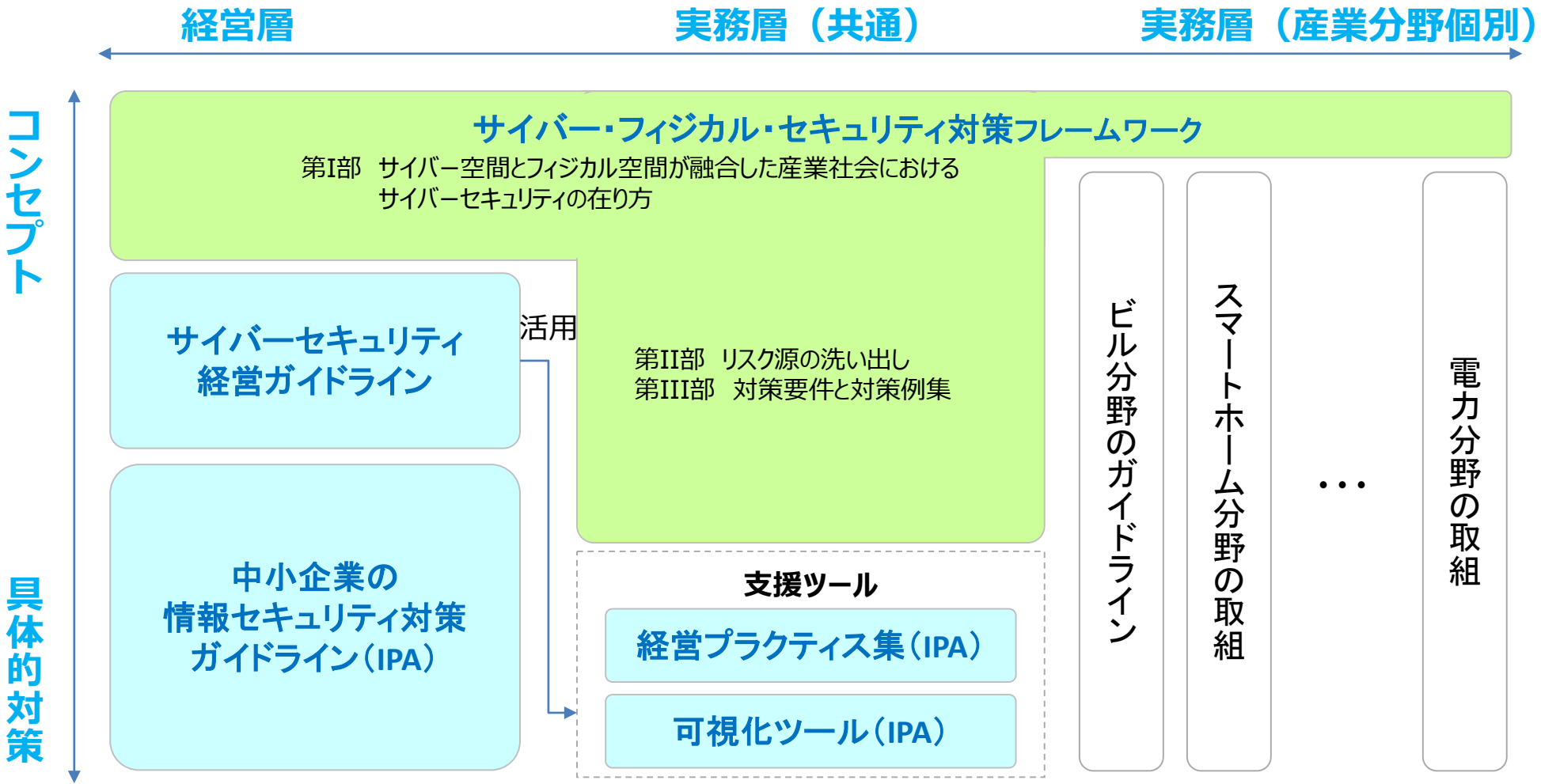
産業サイバーセキュリティ研究会関連の動き



サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

- **「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。**
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞



1．経営

2．人材

3．地域

4．国際

サイバーセキュリティ経営における全体像

第二回WGの再掲

- 経営層向け、現場向け、中小企業向けの３つの視点で、サイバーセキュリティ経営を促進するための施策を検討。

経営層向け

サイバーセキュリティ経営ガイドラインを軸として経営者の意識向上を図るとともに、将来的にセキュリティの高い企業が投資家の評価を受けられる枠組みの構築を支援する。

現場向け

サイバーセキュリティ経営ガイドラインの実践規範となるプラクティスや、対策状況の可視化ツールの提供により対策の実行を支援する。

中小企業向け

サイバー保険との連動も検討しつつ、中小企業におけるセキュリティに関するトラブルの相談対応を支援する。

（１）経営層向けの施策

（２）現場向けの施策

（３）中小企業向けの施策

段階的なサイバーセキュリティ経営の実現

第二回WGの再掲

- 以下の3Stepにより、サイバーセキュリティ経営の定着を目指す。

1st Step

サイバーセキュリティ経営の明確化

- サイバーセキュリティ経営ガイドラインの普及・定着

2nd Step

サイバーセキュリティ経営の実践

- CGS(コーポレート・ガバナンス・システム)ガイドラインにサイバーセキュリティを反映
- IRの観点から、サイバーリスクを経営リスクとして認識・自己確認することの重要性を啓発
- 取締役会実効性評価の項目にサイバーリスクを位置づけ
- 投資家に対してもサイバーセキュリティの重要性を啓発

3rd Step

セキュリティの高い企業であることの可視化

- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

サイバーセキュリティ経営ガイドラインの見直しに向けて
～サイバー・フィジカル・セキュリティ対策フレームワークのコンセプトの反映等

- 産業社会全体におけるリスクを捉えたサイバー・フィジカル・セキュリティ対策フレームワークのコンセプトも踏まえ、経営層のサイバーセキュリティに対する意識の定着を図るために、サイバーセキュリティ経営ガイドラインの改訂を含めた検討を開始する。

課題

インシデントに係る報道により、経営層の意識は高まるものの、一時的なものとなる場合がある

対応

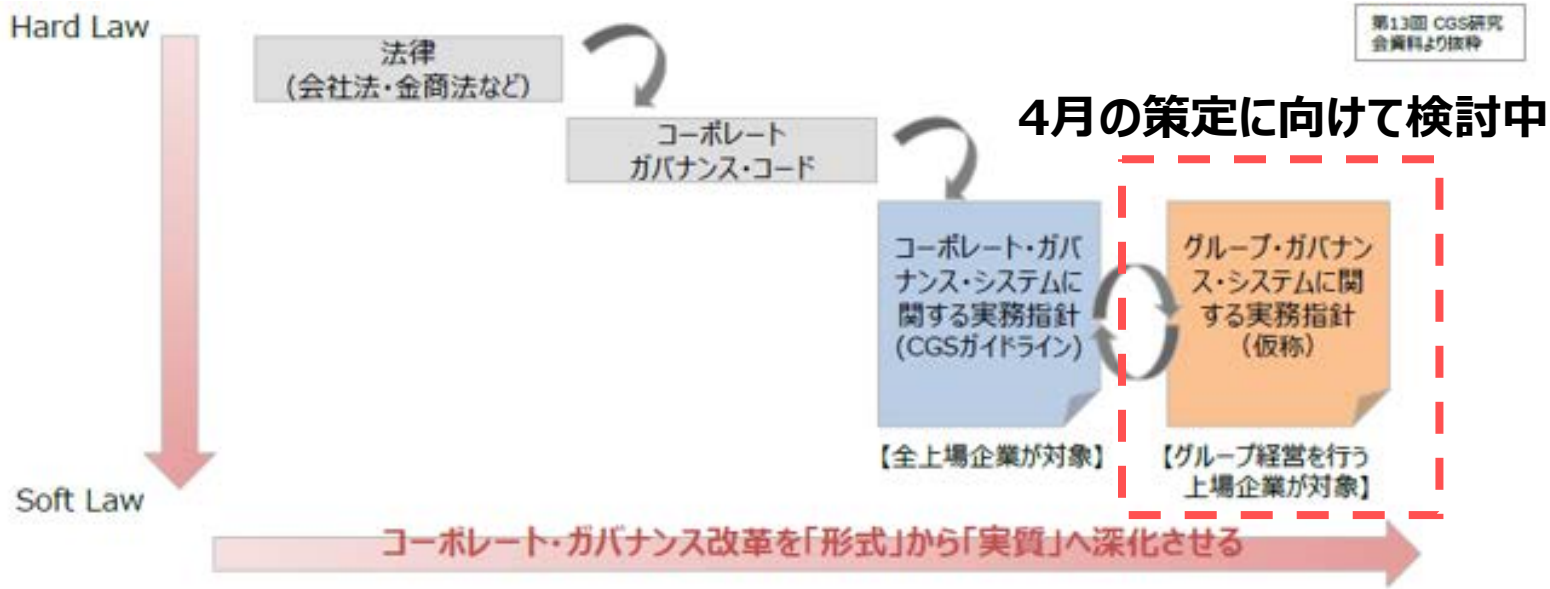
- ◆ フレームワークの考え方をベースとし、サイバーセキュリティ対策が事業継続や新たな価値創出のために不可欠な「投資」と捉える意識改革が必要。
- ◆ 経営ガイドラインにおいて、事業の中での必要性を強くメッセージ出しすることで、一時的な危機意識でなく、恒久的な必要性について認識の促進を目指す

＜サイバーセキュリティ経営ガイドラインの改訂に向けた検討項目＞

- サイバー・フィジカルセキュリティ対策フレームワークをベースとした再整理
- 可視化ツールの作成にあわせて、付録A（サイバーセキュリティ経営チェックシート）の項目を見直し
- 経営者へのメッセージの出し方を見直し（リスクベースの議論だと恒久的な意識が根付かないため）

グループ・ガバナンスシステムに関する実務指針へサイバーセキュリティを位置づけ①
~コーポレートガバナンスコードと実務指針の関係

- 平成29年12月から、CGS研究会（コーポレート・ガバナンス・システム研究会第2期）において、企業グループ全体の価値向上を図る観点からグループガバナンスの在り方を検討。
- 特に、グループ経営を行う上場企業を主たる対象とし、グループ全体の価値向上を図る観点からグループガバナンスの在り方を示す「グループ・ガバナンスシステムに関する実務指針（仮称）」を、平成31年6月を目処に策定予定。



CGS研究会（第2期）＜平成29年12月に第一回を開催し、平成31年3月までに15回開催＞

直近のスケジュール：　第14回（2/12）ガイドライン骨子
第15回（3/15）ガイドラインとりまとめ素案
第16回（4/18）ガイドラインとりまとめ（予定）

グループ・ガバナンスシステムに関する実務指針へサイバーセキュリティを位置づけ②
～サイバーセキュリティ経営を内部統制システムとして明記

- 「グループ・ガバナンス・システムに関する実務指針（仮称）」において、**グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方を位置づけ。**
- 親会社の**取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を行うことを検討すべき**ことを明記。

「グループ・ガバナンス・システムに関する実務指針（仮称）」の目次案

サイバーセキュリティ対策の在り方（案）

- サイバーセキュリティ対策については、内部統制システム上の重要なリスク項目として認識し、サイバー攻撃を受けた場合のダメージの甚大さに鑑み、**親会社の取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を行うことを検討すべきである。**

  実務指針の案より抜粋
- サイバーセキュリティ経営ガイドラインの概要として以下を記載
  - ✓ グループ会社等における対策も、基本的には親会社も責任が問われる。
  - ✓ サイバーセキュリティ経営ガイドラインに従った対応を行うことが重要。
  - ✓ グループ会社等に対策の実施を指示するとともに、着実に対策が実施されていることの確認が重要。
  - ✓ グループ会社等に中小企業がいる場合は、SECURITY ACTIONの宣言の有無を確認することも有効。
  - ✓ 投資家等からの信頼性を高めるために、情報開示を行うことも考えられる。

取締役会実効性評価を通じたサイバーリスクへの対応強化

- コーポレートガバナンス・コードの改訂も受け、「取締役会の実効性評価（コーポレートガバナンス・コード　補充原則4-11③」の実施率は増加傾向にある。
- サイバーリスクに関しては、多くの対応項目の一つ、特にリスク管理として認識が多いものと考えられる。

取締役会の実効性評価の実施状況（東証第一部・第二部上場企業全体）

Power of Equity IR Japan

■ **補充原則4-11③Comply社数　2,061社（78.7%）** 2018年12月31日時点

対象：東証第一部・第二部上場企業のうちCG報告書提出企業数　2,618社

●東証第一部・第二部における実施状況（Complyのうち実施が確認できた1,965社の実施状況）

評価主体	①アンケート	②ヒアリング	③討議	④その他	総計	2018年	2017年
自己評価	1162	155	51	234	1,602	81.5%	82.5%
第三者機関を起用した評価	206	47	4	6	263	13.4%	11.1%
不明	0	0	0	100	100	5.1%	6.3%
総計	1,368	202	55	340	1,965	100.0%	100.0%

●日経平均（日経225）における実施状況（Complyのうち実施予定を除く222社の実施状況）

評価主体	①アンケート	②ヒアリング	③討議	④その他	総計	2018年	2017年
自己評価	95	31	9	13	148	66.7%	74.3%
第三者機関を起用した評価	36	28	2	2	68	30.6%	22.9%
不明	0	0	0	6	6	2.7%	2.9%
総計	131	59	11	21	222	100.0%	100.0%

東証第一部・第二部における第三者評価は昨年から3.3pts上昇の13.4%。日経225企業においては、7.7pts上昇の30.6%となっている。着実に第三者機関を起用した評価の割合が上昇している

コーポレートガバナンス・コード改定への対応

- 政策保有株式
- 後継者計画
- インセンティブ報酬
- CEOの選解任
- 資本コスト

機関投資家からの反対票増加への対応

- 取締役会の多様性
- 業績低迷
- リスク管理（不祥事リスク）

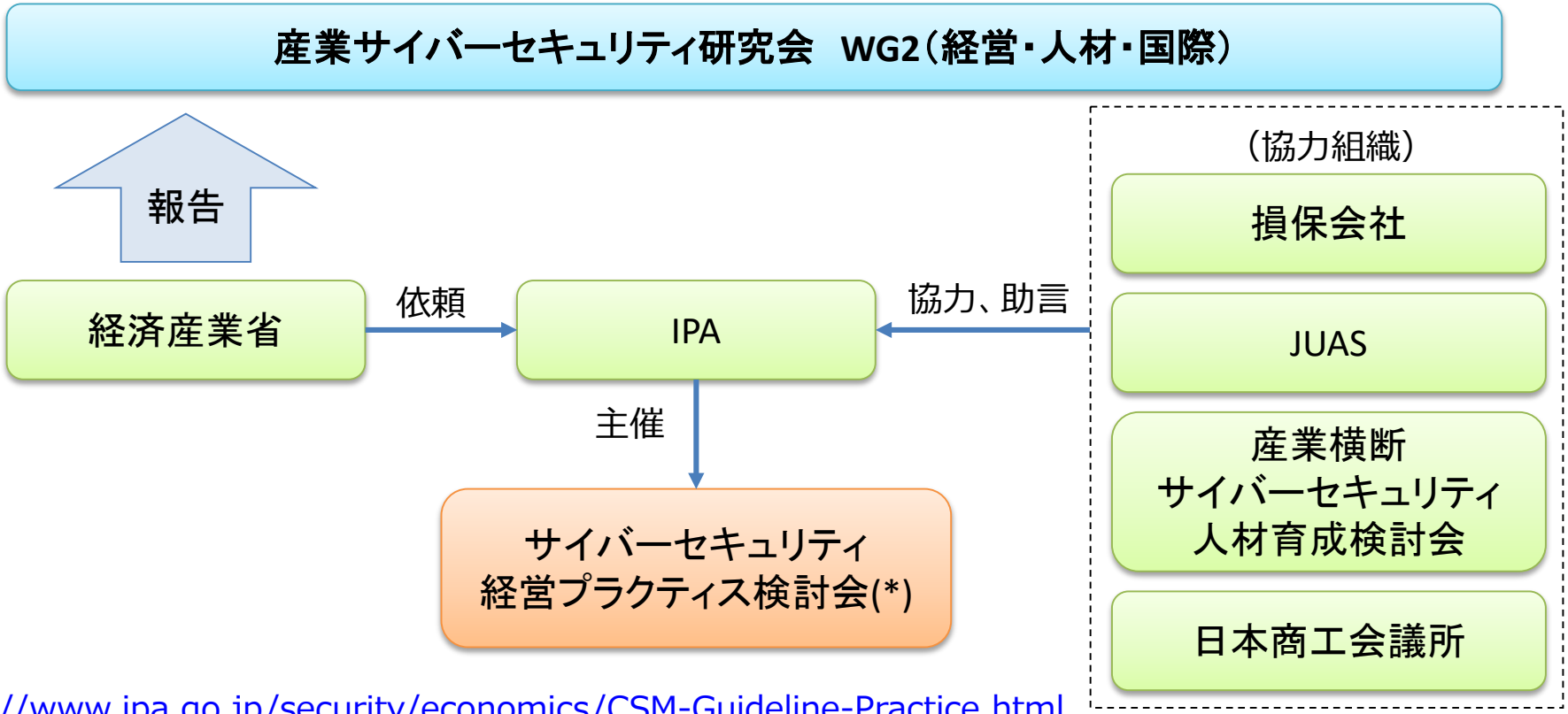
（１）経営層向けの施策

（２）現場向けの施策

（３）中小企業向けの施策

サイバーセキュリティ経営プラクティスと可視化ツールの作成へ向けた検討体制

- **サイバーセキュリティ経営ガイドラインのプラクティス**と、**セキュリティ対策の実施状況を可視化するツールを作成するため**に**サイバーセキュリティ経営プラクティス検討会をIPAに設置**し、全5回開催（平成30年7月～平成31年2月）。



(*) https://www.ipa.go.jp/security/economics/CSM-Guideline-Practice.html

サイバーセキュリティ経営ガイドラインの内容を現場で実現できるよう、『サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集』を策定

- **平成31年3月25日、「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」をIPAから公開。**
- プラクティス集では、サイバーセキュリティ経営ガイドラインの重要10項目の実施に関するプラクティス（第二章）に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示。
- 本プラクティスはJUAS等の業界団体との連携も視野に入れつつ、**継続して収集し、来年度も改訂予定。**

第一章：経営とサイバーセキュリティ

＜経営者、CISO等向け＞
なぜサイバーセキュリティが経営課題となるのか等を解説

第二章：サイバーセキュリティ経営ガイドライン実践のプラクティス

＜CISO等、セキュリティ担当者向け＞
企業の具体事例をベースとした重要10項目の実践手順、実践内容、取り組む際の考え方を解説

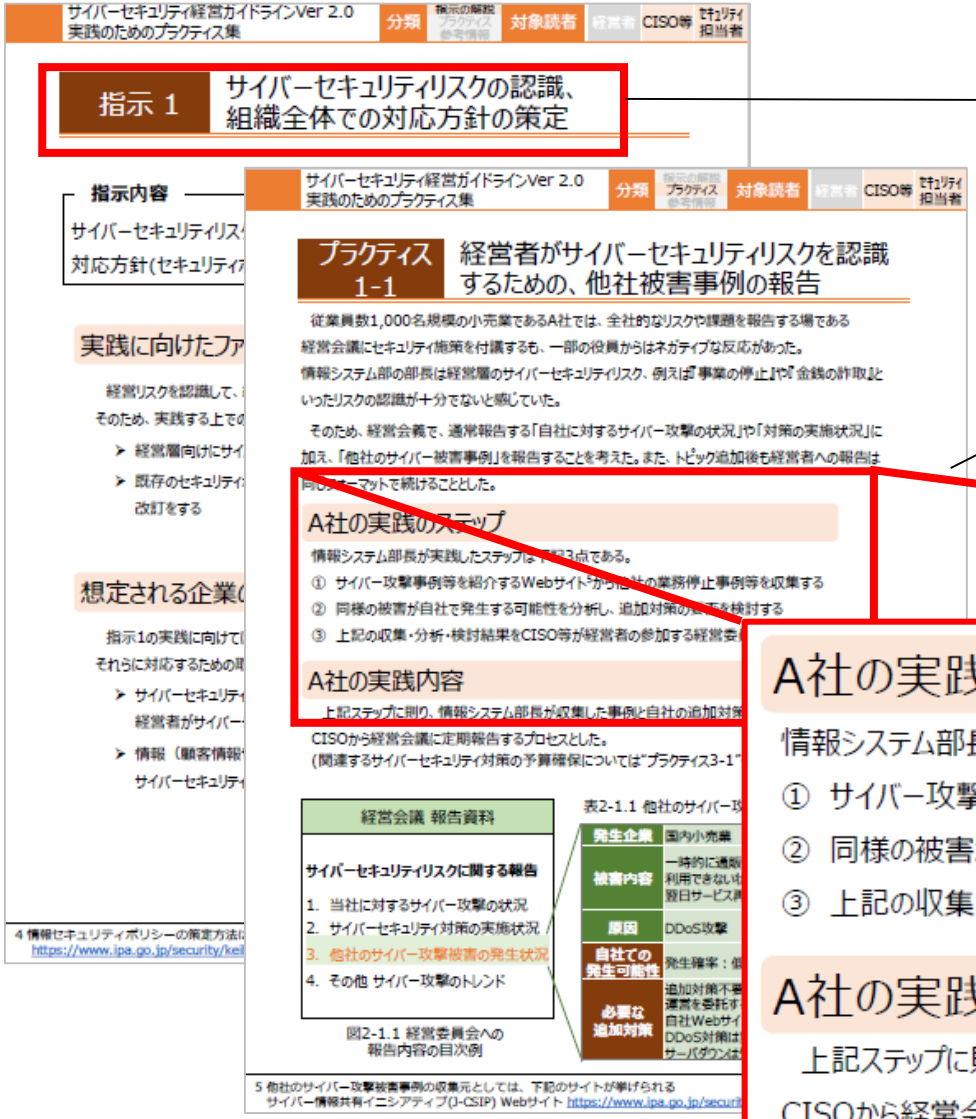
第三章：サイバーセキュリティ対策を推進する担当者の悩みと解決のプラクティス

＜セキュリティ担当者向け＞
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介

＜来年度の方針＞
今年度収集していない以下の指示項目を中心にプラクティスの収集を検討

- 指示4　リスクの把握と対応計画策定
  - リスクアセスメント手法
- 指示6　PDCAの実施
  - リスク管理に関するKPIの定め方
  - 是正措置の実施方法
  - 情報開示の手法
- 指示10　情報共有活動への参加
  - 情報の提供方法
  - 入手した情報の活用方法

プラクティス集（第二章）



サイバーセキュリティ経営ガイドラインの重要10項目毎に章立てを整理

企業の具体的取組をベースに
重要10項目の実践内容を説明

A社の実践のステップ

情報システム部長が実践したステップは下記3点である。

① サイバー攻撃事例等を紹介するWebサイト[5]から他社の業務停止事例等を収集する

② 同様の被害が自社で発生する可能性を分析し、追加対策の要否を検討する

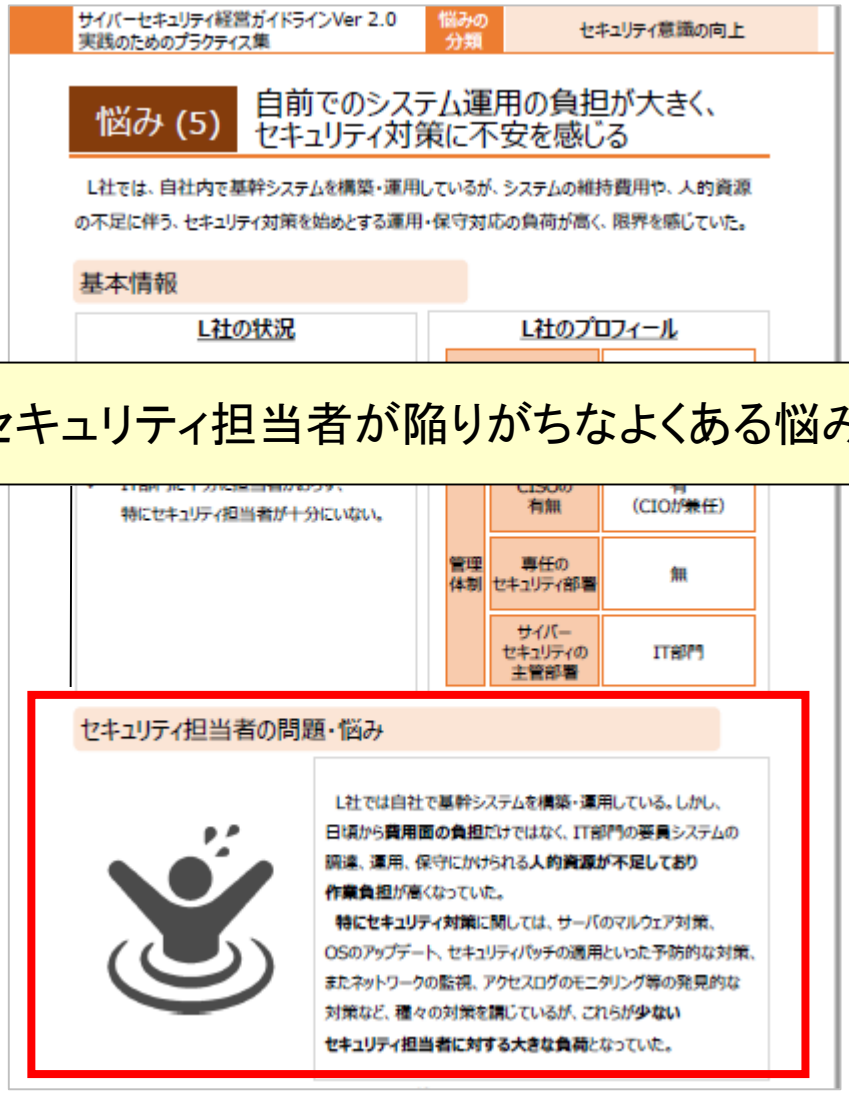
③ 上記の収集・分析・検討結果をCISO等が経営者の参加する経営委員会で定期報告する

A社の実践内容

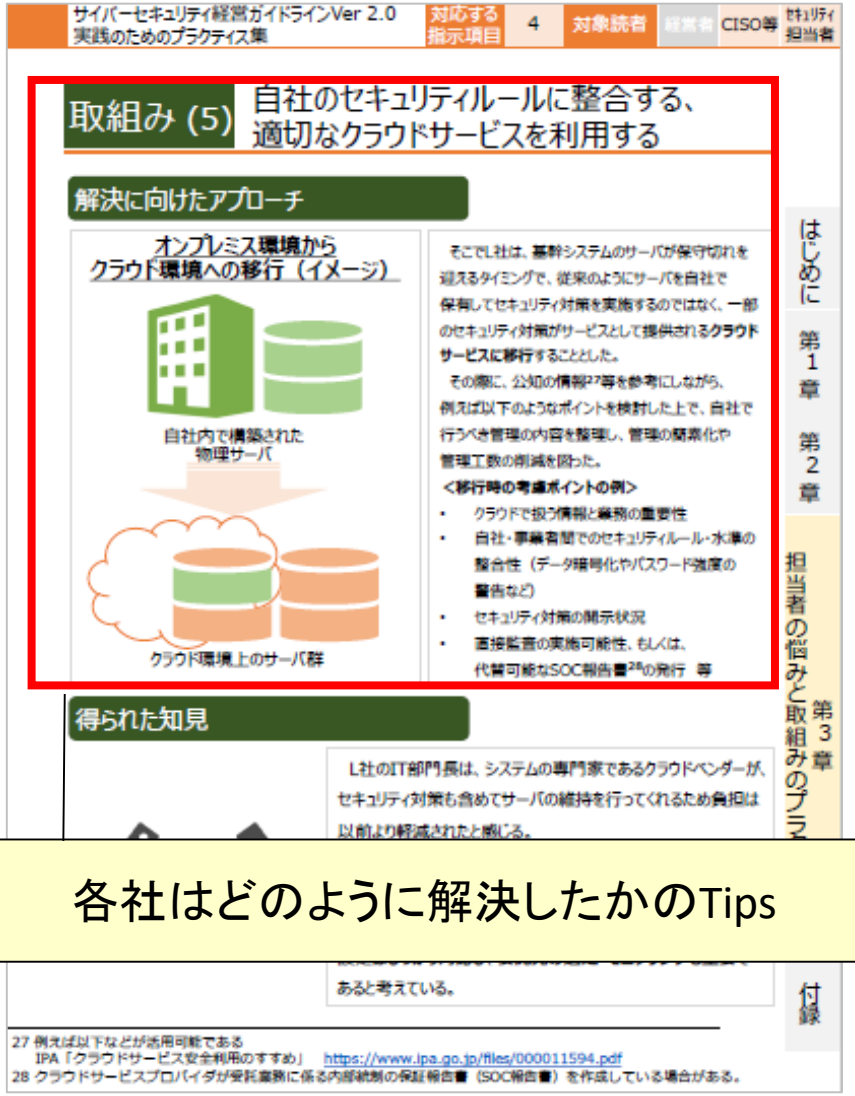
上記ステップに則り、情報システム部長が収集した事例と自社の追加対策要否をCISO等に説明し、CISOから経営会議に定期報告するプロセスとした。

(関連するサイバーセキュリティ対策の予算確保については“プラクティス3-1”を参照)

プラクティス集（第三章）



セキュリティ担当者が陥りがちなよくある悩み

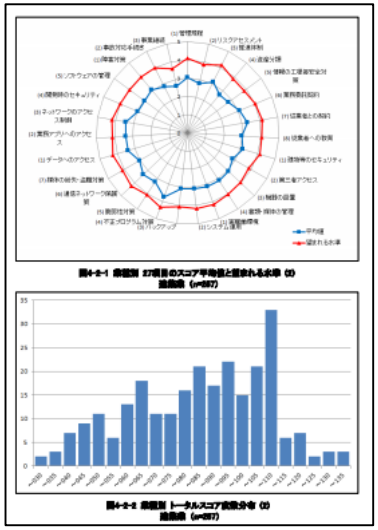


各社はどのように解決したかのTips

可視化ツールの整備：情報セキュリティベンチマークの抜本的な見直し

- 今年度は、Cybermaturity Platform（ISACA）、CAT(*)（FFIEC）等の海外の可視化ツールを調査し、情報セキュリティベンチマーク（IPA）の拡張の可能性を検討。
  - 点数付けの考え方はどのツールも成熟度によっているが、NIST CSFをベースとした海外の可視化ツールはサイバーセキュリティの観点からの設問項目数が充実しているのに対し、ISMSをベースとしている情報セキュリティベンチマークでは、設問項目数がやや少ない。
  - 設問項目について、海外の可視化ツールは粒度が非常に細かいものもあるため、今後作成予定のツールについて、現状の粒度でよいかの議論が必要。
- 来年度、フレームワークや経営GLも参照し、サイバー視点で抜本的な見直しを行う。

＜来年度の可視化ツールの作成の方向性＞



情報セキュリティベンチマーク

セキュリティ視点で
項目追加・見直し

整合性を考慮すべきガイドラインの例

- サイバー・フィジカル・セキュリティ対策フレームワーク（METI）
- サイバーセキュリティフレームワーク（NIST）
- サイバーセキュリティ経営ガイドライン（METI、IPA）

ベンチマークの評価項目と経営ガイドラインを比較し、不足している項目の例
- 経営者がサイバーセキュリティ対策の報告を受けていること
- サイバーセキュリティに関する注意喚起情報等の情報共有、提供を行っていること

(*)FFIEC CAT（FFIEC（米国連邦金融機関検査協議会）が公開するCybersecurity Assessment Tool）

（参考）海外における可視化ツールの例

FFIEC CyberSecurity Assessment Tool

金融機関が自組織におけるサイバーセキュリティの成熟度を自己評価するためのツール。NIST CSFとの整合性を考慮。
5段階の成熟度で評価。

＜設問の例（Intermediate）＞
侵入試験は、繰り返し実施され、中程度、高リスク、悪用可能な脆弱性が解決されたことを確認している。

CREATe Leading Practice for Cybersecurity

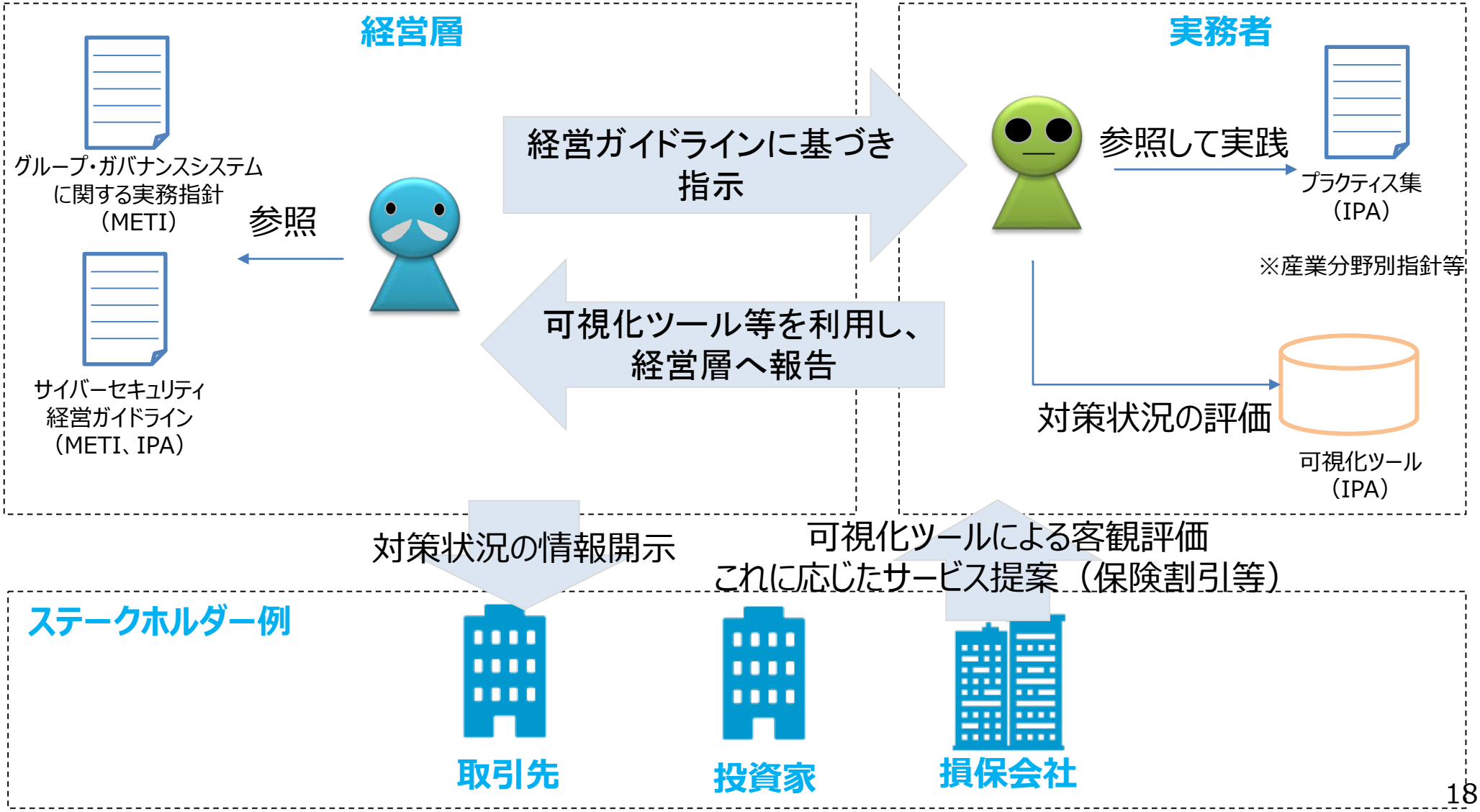
NIST CSFをベースとした自己評価ツール。NIST CSFの主要カテゴリ（特定、防御、検知、対応、復旧）に分類されている詳細項目それぞれに対して、CREATeが独自に考案した設問項目を用意。
5段階の成熟度で評価。
※設問項目等の詳細は非公表のため不明

ISACA Cybermaturity Platform

リスクアセスメント、サイバーセキュリティの成熟度を自己評価するためのツール。
成熟度は、従来のCMMIの評価モデルをベースとしており、5段階で評価。
NISTやISO/IEC27001等の様々な業界標準のフレームワークを参考に設問項目が作成されており、最大で3,100を越える設問項目を用意。

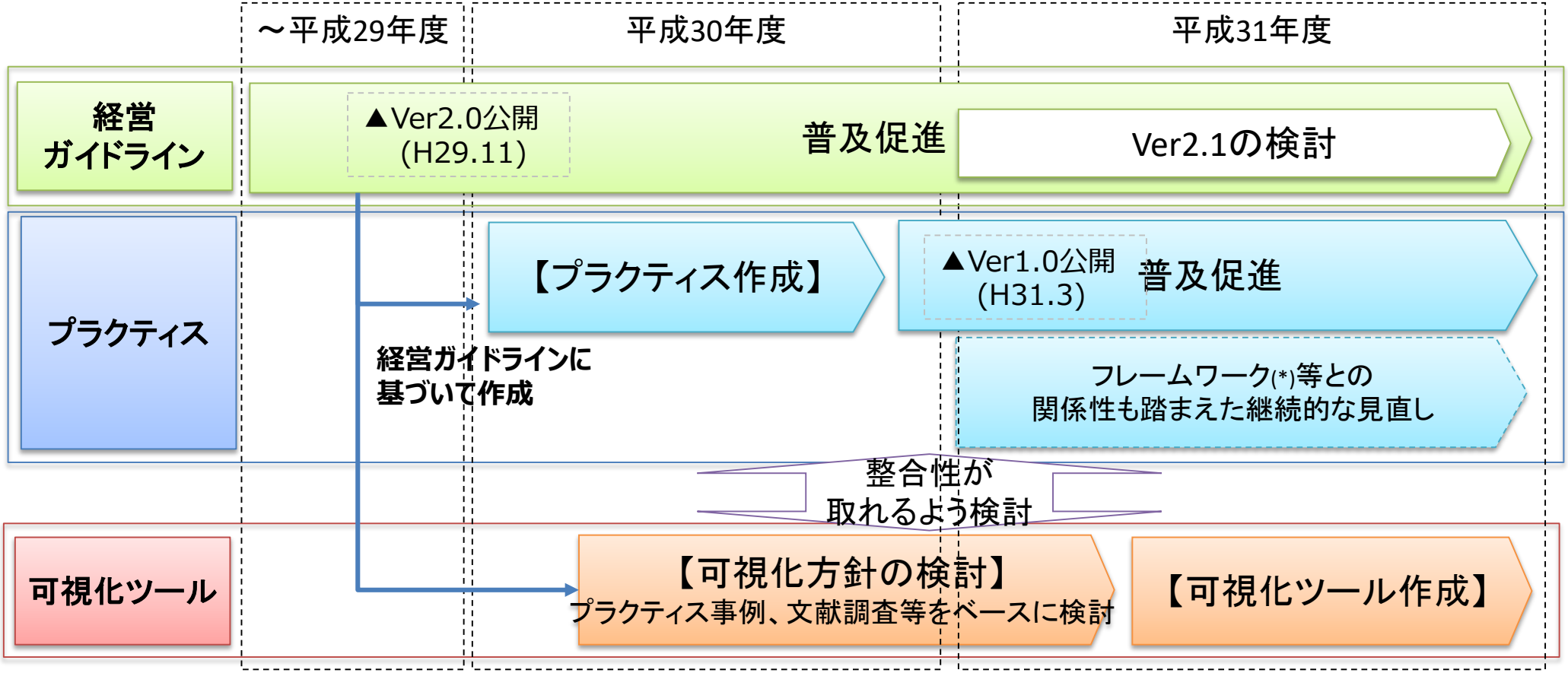
（参考）プラクティス集、可視化ツールの活用例

- 経営ガイドライン、プラクティス集、可視化ツールを活用することで、実践的かつステークホルダーの信頼にも結び付くサイバーセキュリティ経営につながる。



今後のスケジュール

- **サイバーセキュリティ経営ガイドライン、プラクティスの見直し・普及によりサイバーセキュリティ経営の明確化と実践を図る。**
- 可視化ツールの策定を通じ、こうした取組状況を客観的な指標により評価可能とし、**自社の取組状況の確認やステークホルダーによる評価に結びつける。**



(*)サイバー・フィジカル・セキュリティ対策フレームワーク（経済産業省）

（１）経営層向けの施策

（２）現場向けの施策

（３）中小企業向けの施策

中小企業の情報セキュリティ対策ガイドラインの改訂

- 中小企業の経営者やIT担当者が、セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドラインをIPAより公開中。
- パブリックコメント（2019年1月29日～2019年2月8日）の結果を踏まえ修正を行い、第3版（Web版）を**2019年3月19日に公開。**

経営者向けの解説

サイバーセキュリティ経営ガイドラインの内容を中小企業向けに整理し、**経営者が認識すべき３原則と実施すべき重要７項目**を解説

実践者向けの解説

実践者が具体的にセキュリティ対策を実施していくための方法を、**企業のレベルに合わせて段階的にステップアップできる**ような構成で解説

＜主な改訂ポイント＞

- サイバーセキュリティ経営ガイドラインVer2.0との整合性の改善
  （「検知」、「復旧」の観点について、中小企業の実態に即した対応策を提示）
- 中小企業向けに、わかりやすい表現や記述に見直し（第１部　経営者編）
- 組織的な対策の実施体制を、段階的に進めていけるよう構成の見直し（第２部　実践編）
- 「中小企業のためのクラウドサービス安全利用の手引き」を新規追加（付録）

セキュリティ対策自己宣言「SECURITY ACTION」の取得状況 ～IT導入補助金要件化を期に増加

- 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度（IPA）。
- IT導入補助金の申請において、「SECURITY ACTION」の宣言を必須要件化。
- ６万７千者を超える中小企業が宣言（2019年2月末時点）。

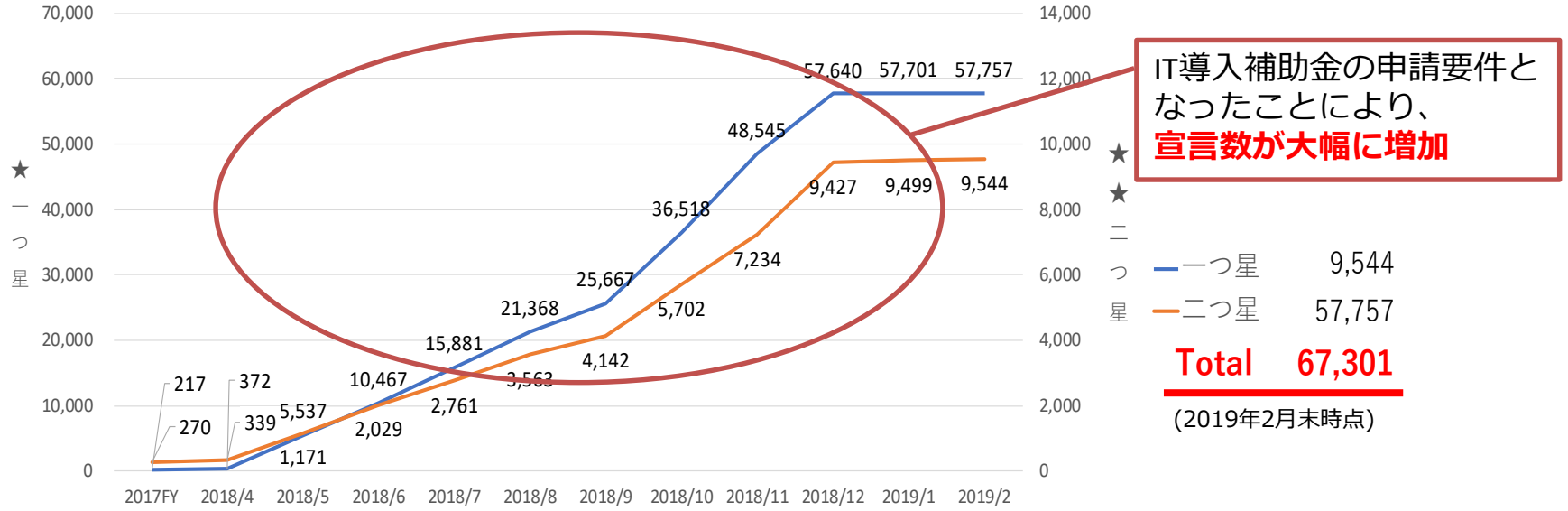
★ 一つ星

情報セキュリティ5か条に取り組む企業

★★ 二つ星

情報セキュリティ自社診断の実施及びセキュリティポリシーを策定する企業

※IPAにて、一般社団法人中小企業診断士協会、全国社会保険労務士会連合会、全国商工会連合会、全国中小企業団体中央会、特定非営利活動法人日本ネットワークセキュリティ協会、特定非営利活動法人ITコーディネータ協会、独立行政法人中小企業基盤整備機構、日本商工会議所、日本税理士会連合会と連携した普及促進活動を実施



「SECURITY ACTION」普及に向けた取組例：～IT導入補助金との連携

- 「SECURITY ACTION」の一つ星または二つ星を宣言することが、IT導入補助金（平成29年度補正）補助申請の要件化。
- IT導入補助金については、３０年度補正事業においても要件化に向け検討中。さらに、今年度も他の補助金を含め、要件化できないか検討中。

平成２９年度補正

サービス等生産性向上

公募要

（第一次

平成３０年（２０１

サービス等生産性向上Ｉ

（一般社団法人 サービス

３．補助事業者の要件

３－１　申請要件

本事業の補助対象者は、次のすべての要件に該当する者に限る。

（１）生産性の向上に資するＩＴツールを導入する中小企業・小規模事業者等であること（中小企業・小規模事業者等の定義については次頁の表を参照）。ただし、次の①～③のいずれかに該当する者は、大企業とみなして補助対象者から除く。

①発行済株式の総数又は出資価格の総額の２分の１以上を同一の大企業が所有している中小企業・小規模事業者等

②発行済株式の総数又は出資価格の総額の３分の２以上を大企業が所有している中小企業・小規模事業者等

③大企業の役員又は職員を兼ねている者が、役員総数の２分の１以上を占めている中小企業者

（２）日本国内で事業を行う個人又は法人であること。

（３）風俗営業等の規制及び業務の適正化等に関する法律第２条に規定する「風俗営業」、「性風俗関連特殊営業」及び「接客業務受託営業」を営むものでないもの。ただし、旅館業法（昭和２３年法律第１３８号）第３条第１項に規定する許可を受け旅館業を営むもの（風俗営業等の規制及び業務の適正化に関する法律（昭和２３年法律第１２２号）第２条第６項に規定する店舗型性風俗特殊営業を営むものを除く。）を除く。

（４）申請者（中小企業・小規模事業者等）又はその法人の役員が、暴力団等の反社会的勢力でないこと。反社会的勢力との関係を有しないこと。また、反社会的勢力から出資等資金提供を受けている場合も対象外とする。

（５）申請者（中小企業・小規模事業者等）の労働生産性(※1)について、補助事業を実施することによって３年後の伸び率１%以上、４年後の伸び率１．５%以上、５年後の伸び率２%以上又はこれらと同等以上の生産性向上を目標とした計画を作成すること。原則として、労働生産性の向上を目標とした計画及び導入するＩＴツールによる生産性向上指数に類する独自の数値目標(※2)を作成すること。

（※1）労働生産性とは、粗利益（売上-原価）／（従業員数×１人当たり労働時間（年平均））により算出された値を言う。

（※2）独自の数値目標例：従業員あたり顧客数、従業員あたりの外国人客数、営業員あたりの取引業者数、営業員あたりの取引品目数、従業員あたり診療報酬点数等、従業員あたり製造量又は生産量、時間あたりの顧客数（配送数・接客数等）等

（６）独立行政法人情報処理推進機構（IPA）が実施する「SECURITY ACTION」の「★ 一つ星」または「★★ 二つ星」いずれかの宣言を行うこと。また、宣言内容の確認に際し事務局が一部の交付申請情報を独立行政法人情報処理推進機構（IPA）と共有することに同意すること。

（７）補助金交付申請内容については、「ＩＴ導入支援事業者を含む“第三者”による総括的な確認」を受けること。

（８）ＩＴ導入支援事業者を通じて、生産性向上に係る情報（売上、原価、従業員数及び就業時間）等を事務局に報告すること。

（９）補助事業に係るすべての情報について、事務局から国に報告された後、統計的な処理等をされて匿名性を確保しつつ公表される場合があることについて同意すること。

6

３－１　申請要件

本事業の補助対象者は、次のすべての要件に該当する者に限る。

（中略）

（６）独立行政法人情報処理推進機構（IPA）が実施する「SECURITY ACTION」の「★ 一つ星」または「★★ 二つ星」いずれかの宣言を行うこと。また、宣言内容の確認に際し事務局が一部の交付申請情報を独立行政法人情報処理推進機構（IPA）と共有することに同意すること。

～IT導入補助金公募要領より抜粋～

中小企業支援団体との連携の強化

- IPAにおいて四半期に一度、**中小企業のサイバーセキュリティ対策を支援に関わる団体が一堂に会し、中小企業の情報セキュリティ普及推進協議会を開催。**
  「SECURITY ACTION」を始めとした、中小企業向け施策について議論。
- **協議会参加団体も、積極的に中小企業のセキュリティ意識向上に向けた取組を実施。**

日本商工会議所

- 商工会議所イントラネットシステム、研修会、会議等での周知
- イントラネットシステムを通じた、「5分でできる！自社診断シート」の一斉実施
  （全国515中、485商工会議所（94%）が実施、採点）
  ⇒結果、**約180商工会議所がSECURITY　ACTIONを取得**
- 会員企業向けに発行する「会議所ニュース」にて、IPAと協力し、セキュリティ特集記事を継続して掲載。

ITコーディネータ協会

- 「講習能力養成セミナー」をIPAと共催（全国12地域）
- 「IT導入補助金支援者向け説明会」を開催：補助金導入支援者にSECURITY ACTION制度を説明
- 「SECURITY ACTION普及支援モデル」を試行：3日間訪問モデル（ミラサポを活用した3日間の無料支援）と題し、**ITCによるSA取得支援活動を実施し、一定の成果を得た。**

中小企業の対策強化に向けた面的な取組～中小企業等強靭化対策事業

- 平成30年度第二次補正予算、中小企業強靭化対策事業の施策として、「セキュリティマネジメント指導業務」及び「サイバーセキュリティお助け隊」の実証事業を実施（15.0億円の内数）。
- 本事業により、**事前、事後のサプライチェーンセキュリティ対策を一体で促進**する。

サプライチェーンセキュリティ対策促進

事前対策としての意識向上・対策相談、事後対策としてのお助け隊を両輪で進め、面的な取組を強化

主に事前支援（セキュリティマネジメント指導業務）

＜目的＞中小企業が具体的な対策を実践する際に、気軽に相談できる専門家を派遣することで、セキュリティの意識向上、事前セキュリティ対策水準向上につなげる。

実施体制

IPA

①講師の育成、指導
中小企業向けセキュリティマネジメント指導に必要なガイドを学習するための講師の育成、指導

情報処理安全確保支援士

②事業の周知、募集、受付
・お助け隊事業の説明会における周知
・SECURITY ACTION宣言事業者（一つ星）へ呼びかけ
・ミラサポメルマガ等での呼びかけ 等

中小企業
特に重要インフラ関連企業のサプライチェーンに属する企業

③セキュリティマネジメント指導
・事前対策に関する支援を実施。
・主にセキュリティポリシー策定を支援
・1社当たり4回、専門家を派遣

事前対策促進

主に事後支援（サイバーセキュリティお助け隊）

＜目的＞中小企業がサイバー攻撃等で困った際に相談し、対応する窓口を創設。セキュリティ意識向上を図ると共に、サイバー攻撃の実態や事後対策ニーズを図り、中小企業が利用し易い支援サービスの構築につなげる。

実施体制

保険会社

中小企業への周知、集客
・商工会議所、重要産業の大企業、地域経産局等との連携
・説明会の実施

①相談
＜電話orメール＞

②対応
＜可能な場合＞

③対応依頼
＜対応困難な相談の場合＞

機器設置

中小企業
特に重要インフラ関連企業のサプライチェーンに属する企業

④インシデント判断、対応
＜必要に応じて駆付け＞

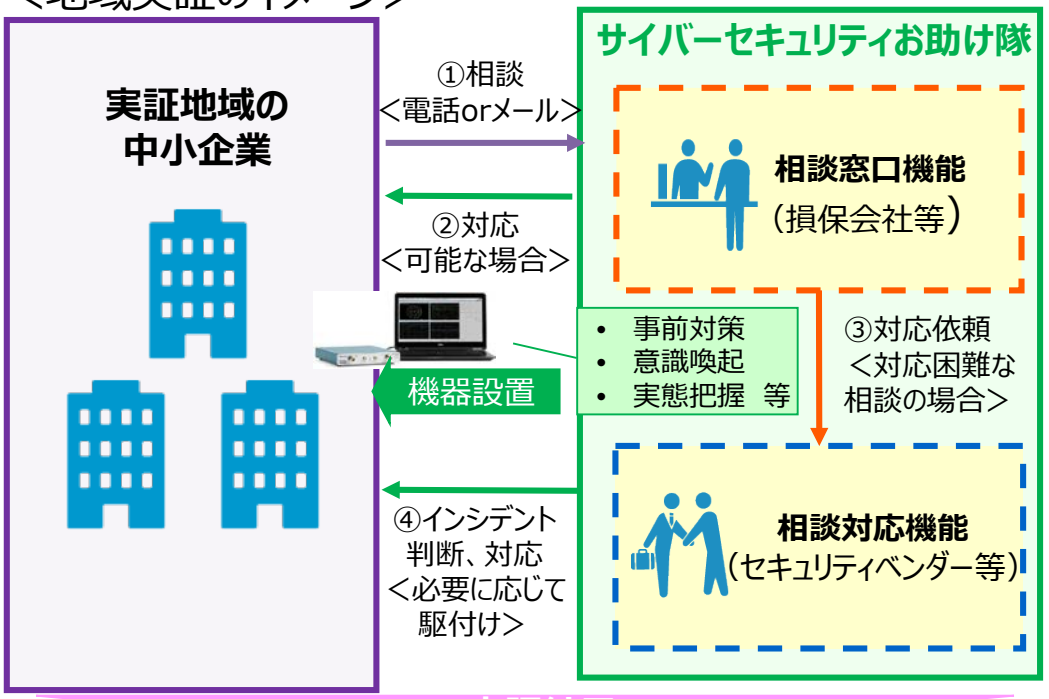
セキュリティベンダー

事後対策促進

サイバーセキュリティお助け隊の実証
～中小企業を面的に支援する体制の構築へ向けて

- 中小企業向けにサイバーセキュリティに関する支援の仕組みを新たに構築し、全国最大**8地域**を対象に地域の団体、企業等と連携した**実証**を行い、**サイバー攻撃の実態や対策のニーズを把握するとともに、中小企業の事前対策の促進、意識喚起を図る。**

＜地域実証のイメージ＞

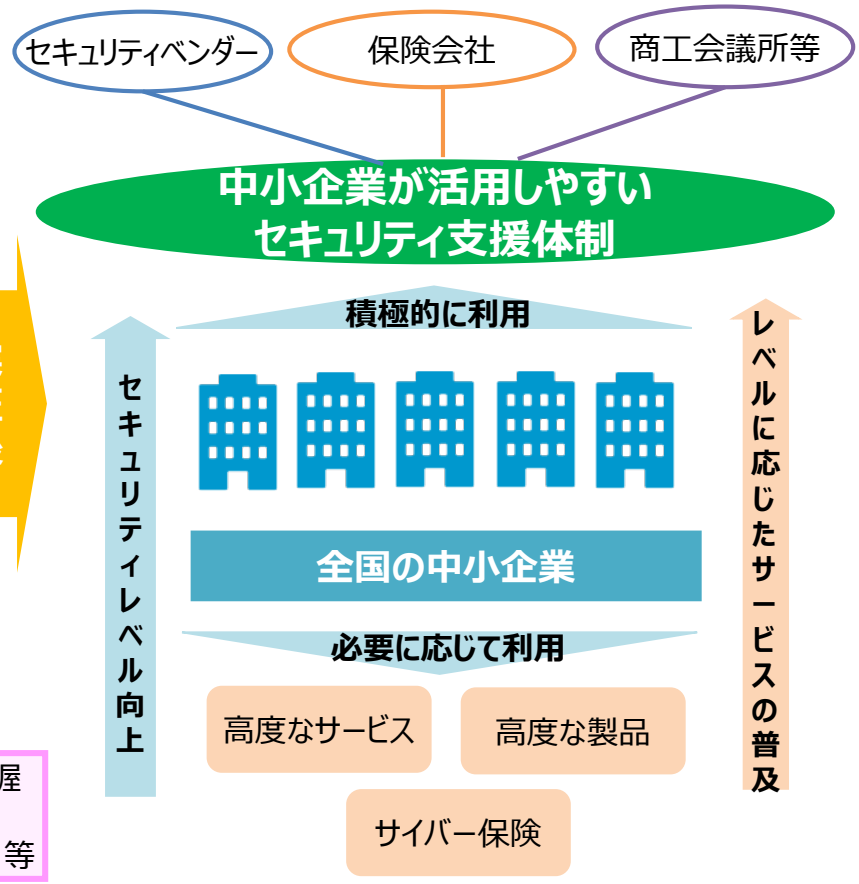


実証結果

中小企業 側
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上 等

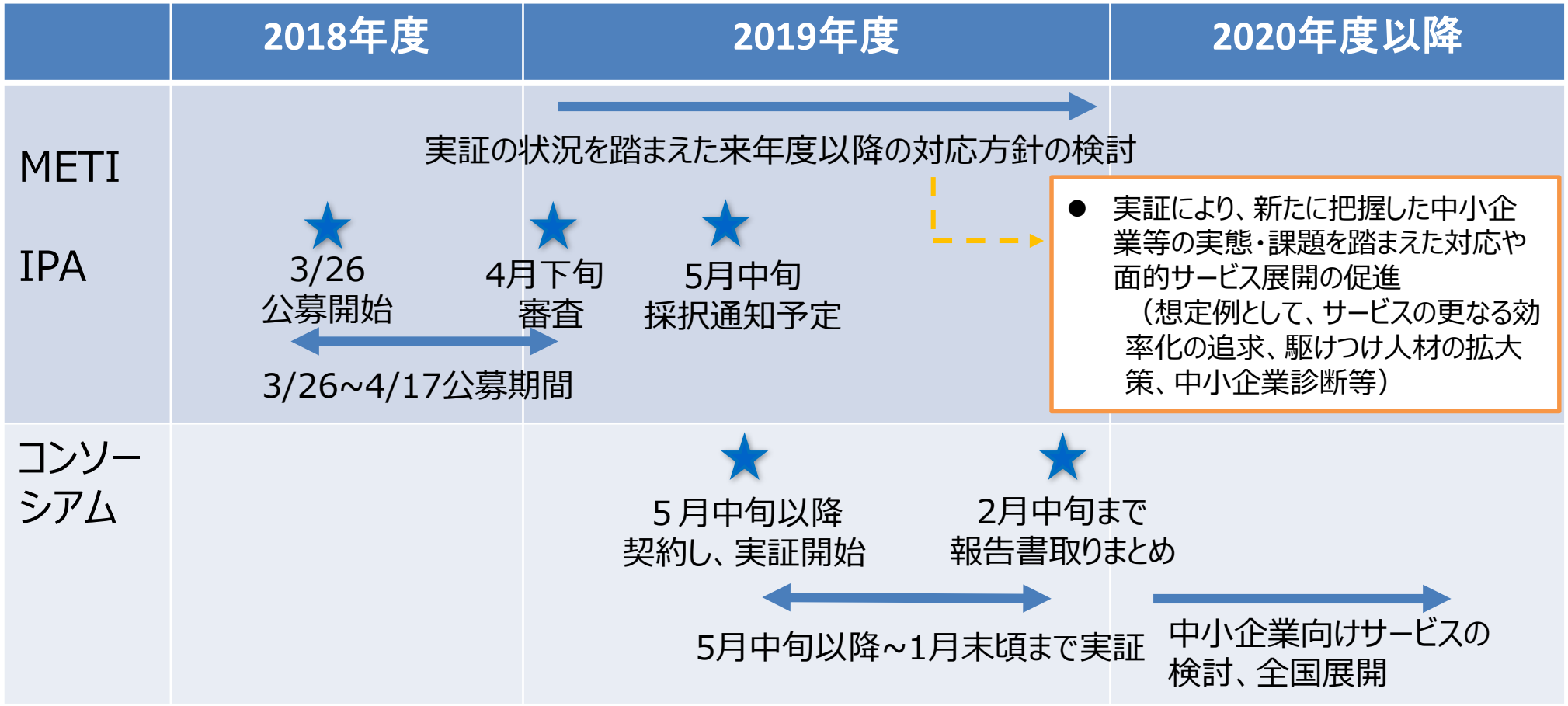
保険会社、セキュリティベンダー 側
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握 等

実証後



サイバーセキュリティお助け隊（スケジュール）

- IPAが事業実施主体となり、3月26日から公募を開始。コンソーシアム単位で全国で実証事業を行う。あわせて、実証を通じ中小企業の実態把握を深め、実態に応じた効果的な取組も検討していく。



1．経営

2．人材

3．地域

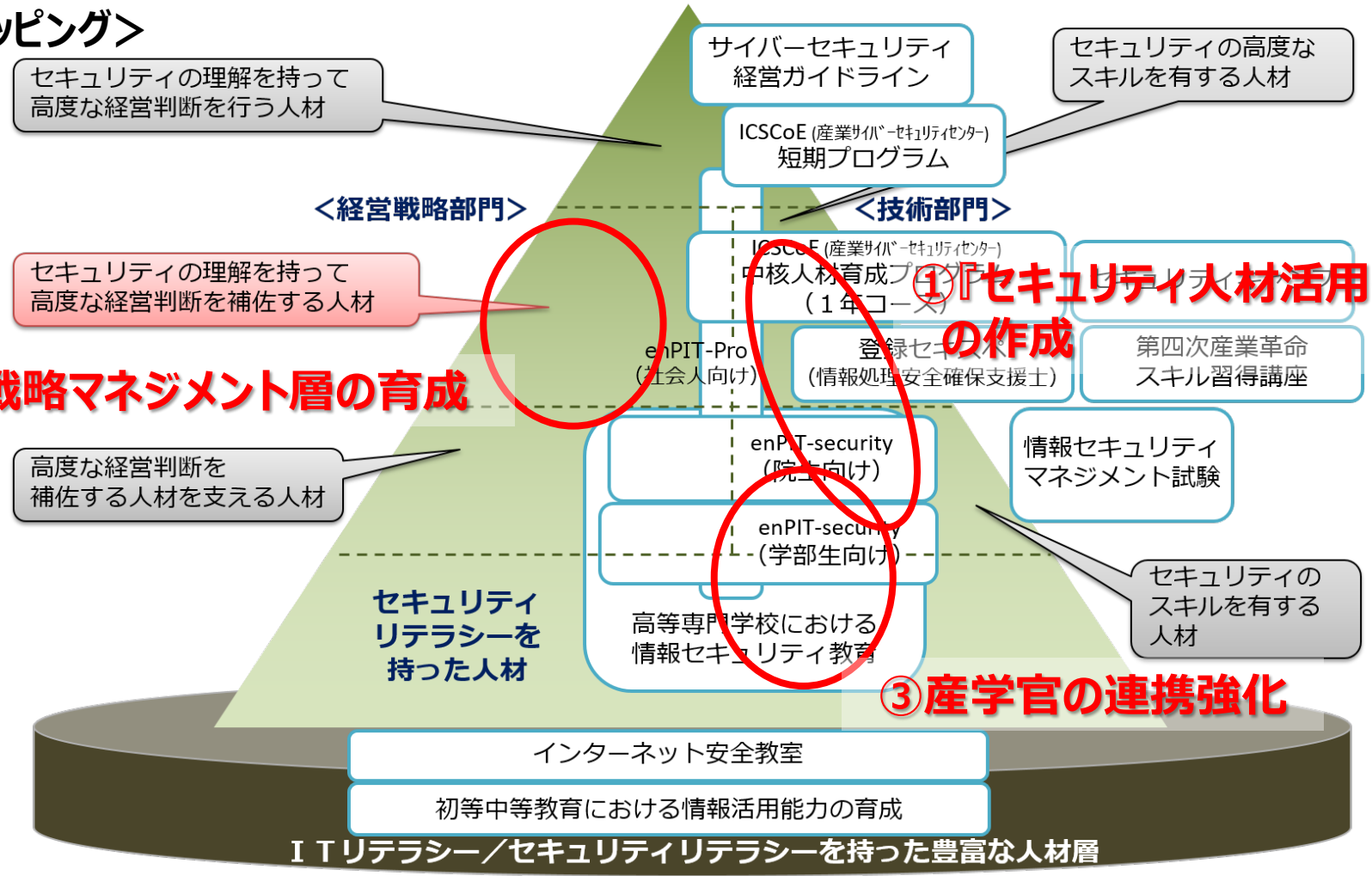
4．国際

サイバーセキュリティ人材育成・活躍促進パッケージの全体像

第二回産業サイバーセキュリティ研究会資料より再掲

- ユーザー企業において必要となる**セキュリティ人材の定義、評価指標が不明確。**
- **「セキュリティの理解を持って高度な経営判断を補佐する人材」の育成が不十分。**
- 教育プログラム策定への貢献など、**産業界の教育への取組の強化が期待される。**

＜政策マッピング＞



（１）『セキュリティ人材活用モデル』の構築

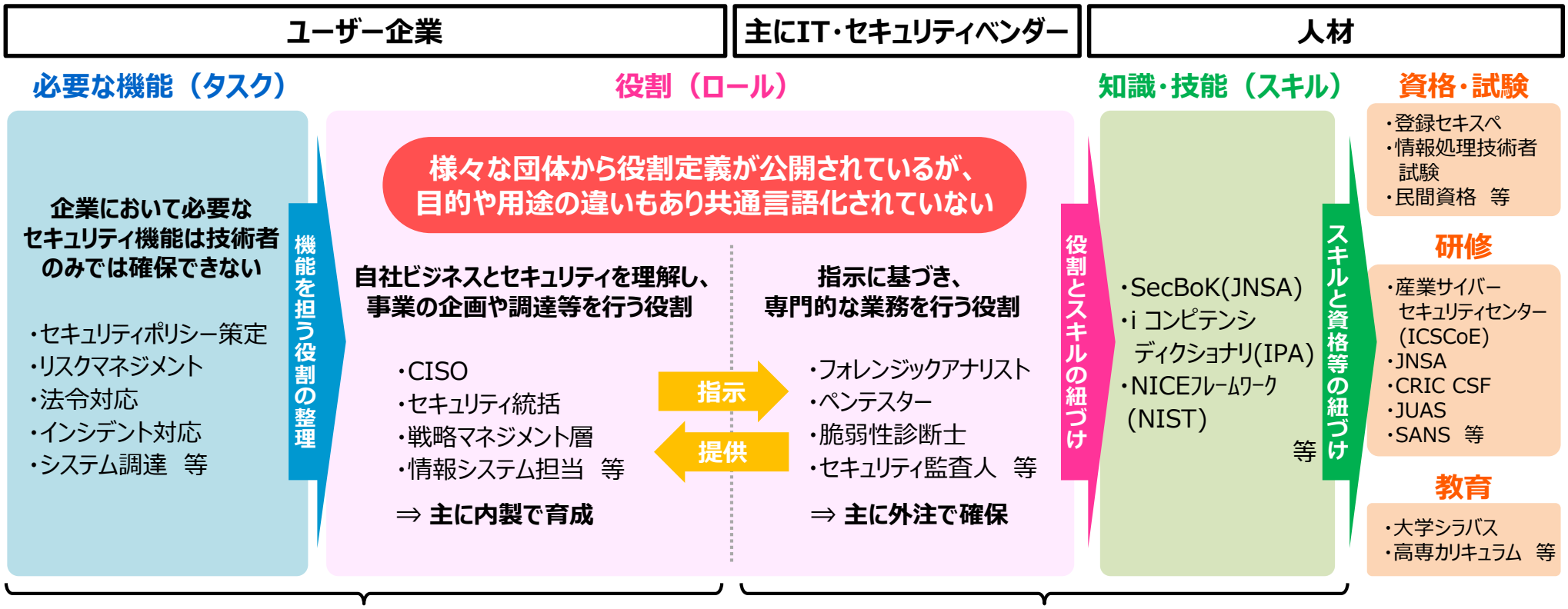
（２）戦略マネジメント層の育成

（３）産学官の連携強化

セキュリティ人材の流動化に対応できる『セキュリティ人材活用モデル』の構築

第3回WGG2資料より

- 企業に求められるセキュリティ機能を果たす人材の役割を、必要な知識・技能（スキル）と紐づけ、共通言語化することにより、人材の雇用・配置・外注等における企業と人材の間のコミュニケーションコストを減らし、マッチングを促進。
- 人材のニーズとシーズの見える化により、セキュリティ人材の最適活用、処遇改善につなげる。



論点1　ユーザー企業によって機能・体制・役割の在り方は様々

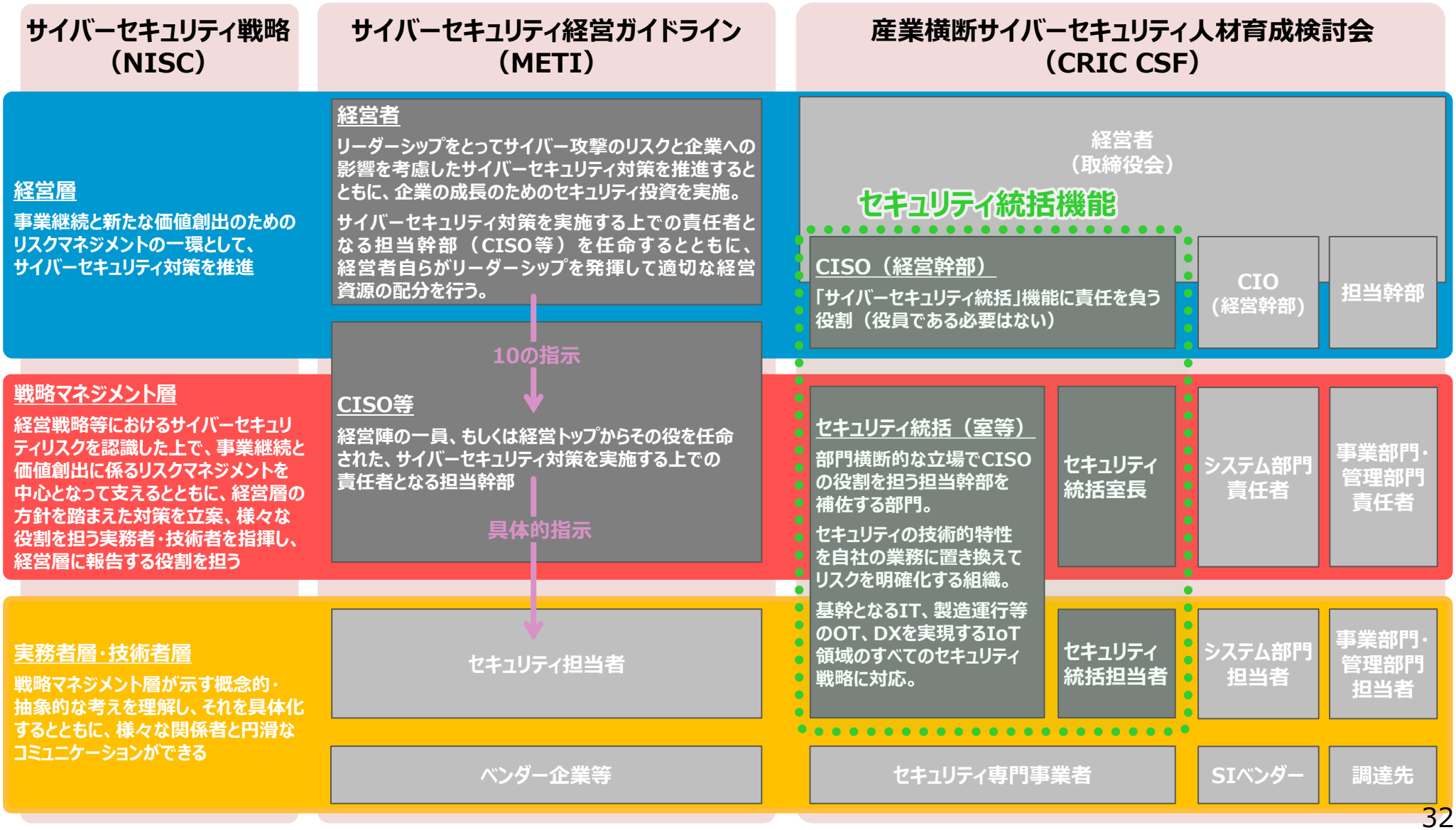
⇒ ユーザー企業の規模・業種・成熟度等に応じたセキュリティ体制や人材確保の関係について調査を実施

論点2　専門性が高い役割は比較的共通言語化しやすい

⇒ SecBoK(JNSA)、ITSS+(METI/IPA)、統合セキュリティ人材モデル(サイバーセキュリティ人材育成スキーム策定共同プロジェクト)等における既存の役割定義・専門分野の関係を整理・明確化

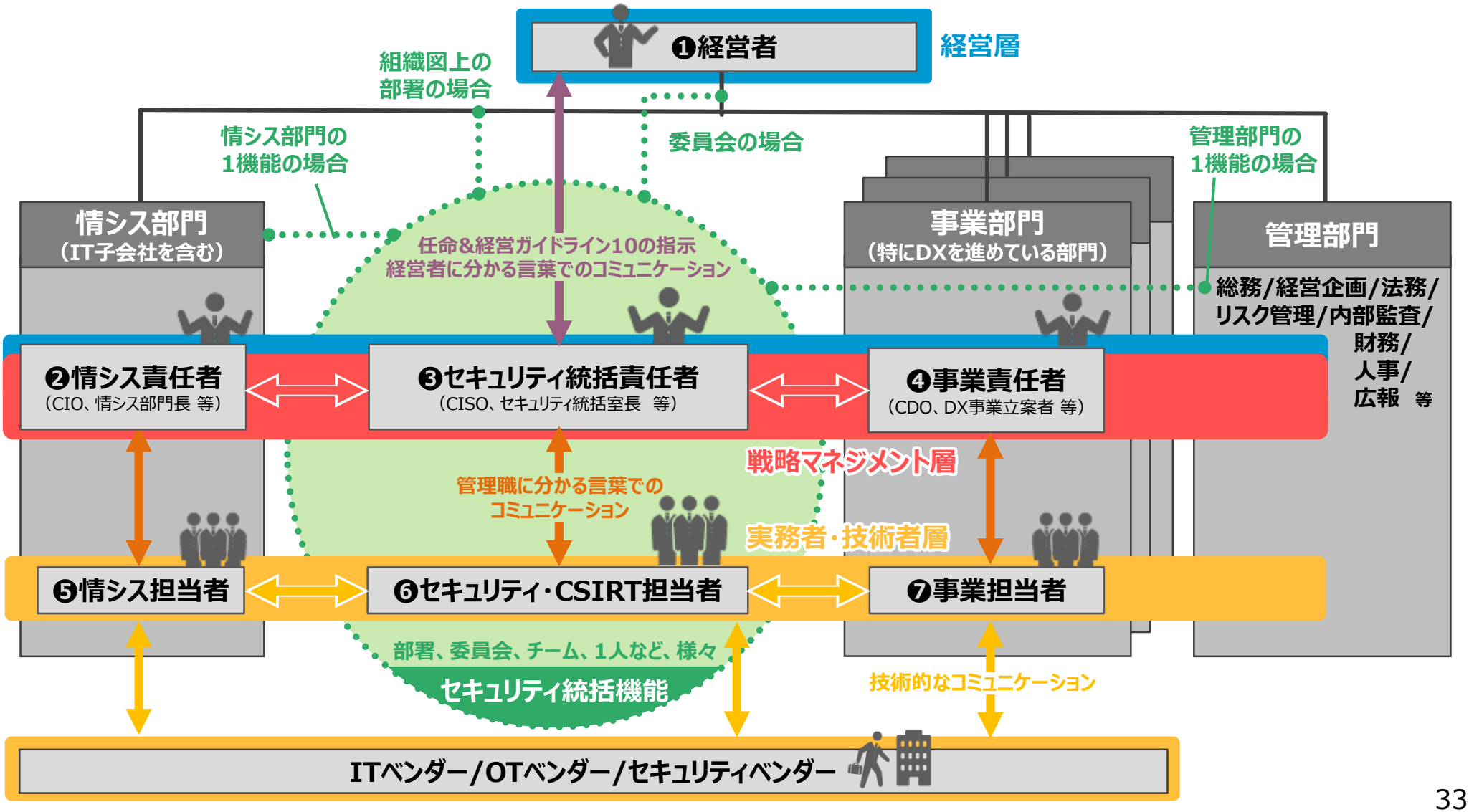
（論点１：ユーザー企業）セキュリティ体制・人材に関する概念整理①

- サイバーセキュリティ戦略における「経営層、戦略マネジメント層、実務者層」、METIのサイバーセキュリティ経営ガイドライン、CRIC CSFの「セキュリティ統括機能」等の諸概念の関係は、以下のように整理できる。



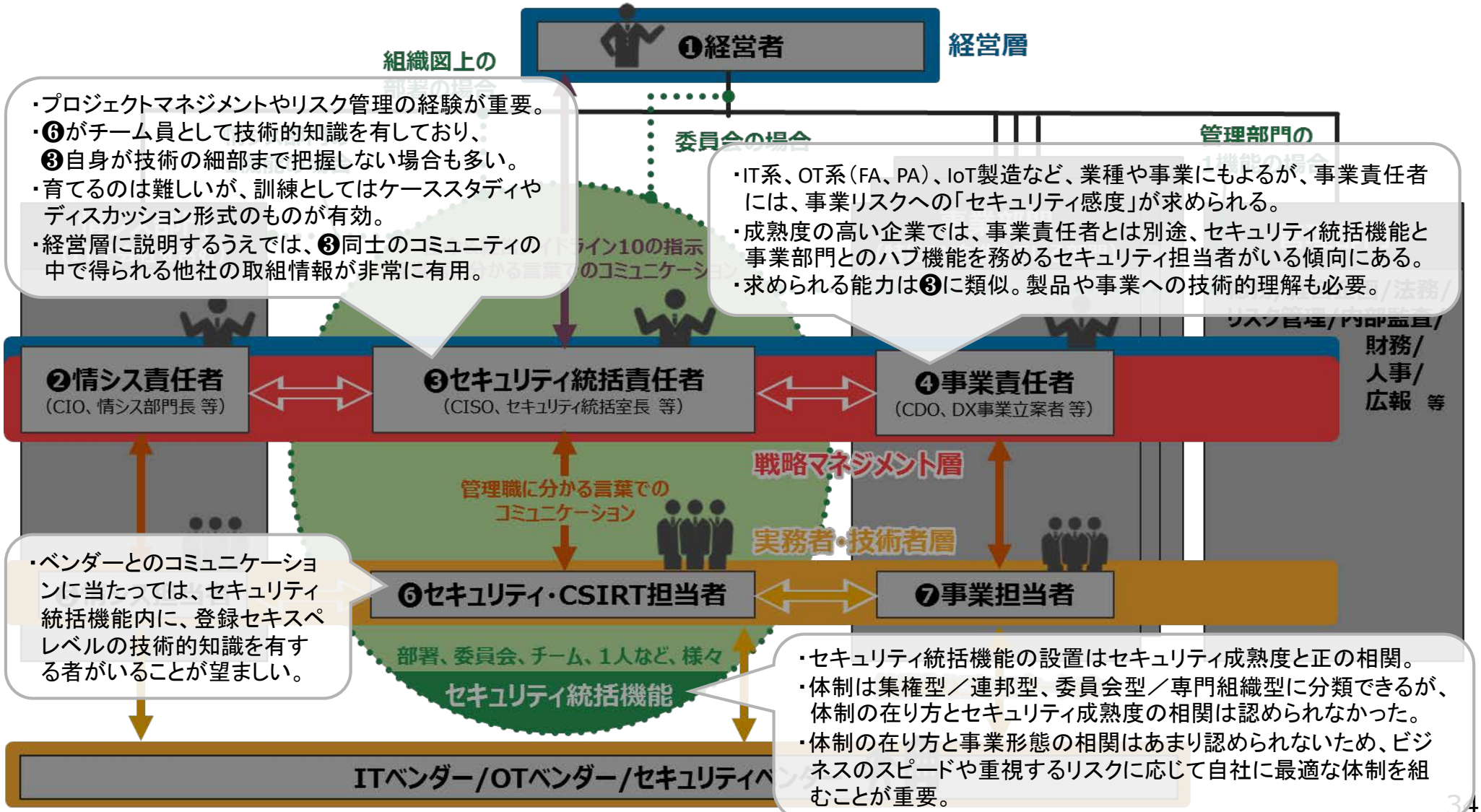
（論点１：ユーザー企業）セキュリティ体制・人材に関する概念整理②

- NISC、IPA、CRIC CSF、JNSA、JUASとの議論を踏まえ、ユーザ企業における諸概念を図式的に整理。



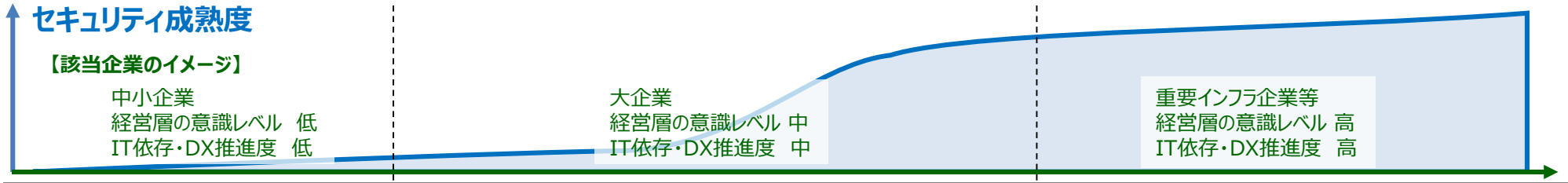
（論点１：ユーザー企業）セキュリティ体制・人材に関する調査

- 今年度、下図のセキュリティ統括機能や戦略マネジメント層等についての委託調査をJUASが受託・実施。
- 72社にアンケートを実施し、31社にヒアリングを実施。（※ 調査結果の詳細は資料５を参照。）

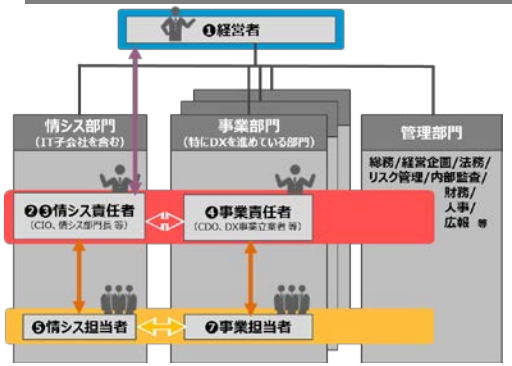


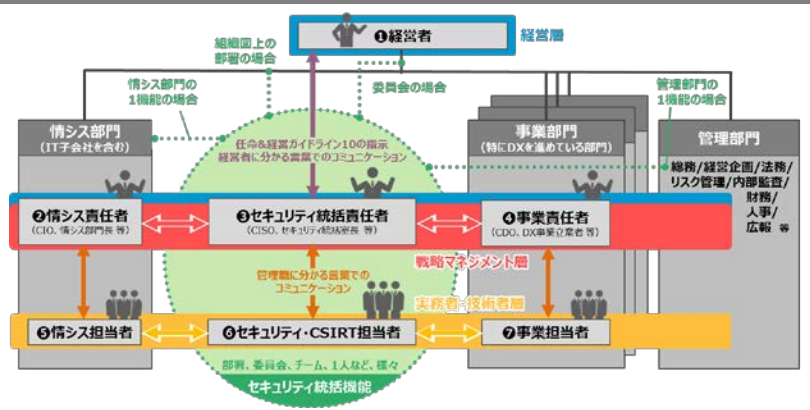
（論点１：ユーザー企業）セキュリティ体制・人材とセキュリティ成熟度の関係整理

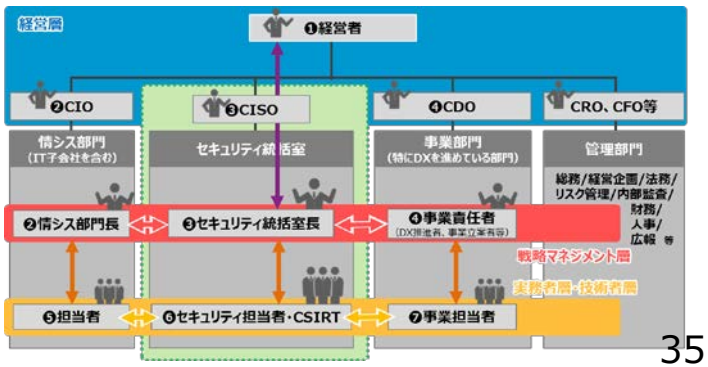
- セキュリティ体制・人材と、セキュリティ成熟度の間には、概ね以下のような関係が認められるのではないか。
- 31年度には、各成熟度段階の企業に参考となるセキュリティ体制・人材確保のためのプラクティスを取りまとめる。



CSIRT機能の設置・確立状況		
△ （→ 窓口の設置を目指す）	○ （→ CSIRTの設置を目指す）	◎ （→ CSIRT機能の確立を目指す）
セキュリティ統括責任者（CISO等）の設置状況		
△ （ → 兼務による担当者設置を目指す）	○ （→ 専任による部課長級の設置を目指す）	◎ （→ 役員級のCISOの設置を目指す）
セキュリティ統括機能の設置・確立状況		
×	○ （→ 設置を目指す）	◎ （→ 機能の確立を目指す）
事業部門・管理部門のセキュリティ意識・能力		
×	△ （→ セキュリティ統括機能との連携を目指す）	○ （ → 事業部門・管理部門の意識・能力の向上を目指す）
体制のイメージ		







（論点２：専門人材）専門性が高い分野における既存の役割定義

- 専門性が高い分野では、目的や用途に応じた様々な役割定義が存在。

＜各団体による役割・専門分野の定義の例＞

ITSS+ (**セキュリティ領域**) 【METI / IPA】	SecBoK 2019 【JNSA】	**人材定義リファレンス** 【CRIC CSF】	**統合セキュリティ人材モデル** **【サイバーセキュリティ人材育成スキーム策定共同プロジェクト】**	NICE**フレームワーク** (Specialty Areas)【NIST】
情報リスクストラテジ	CISO	CISO/ CRO/ CIO等	セキュリティコンサルタント	Risk Management
情報セキュリティデザイン	POC (Point of Contact)	サイバーセキュリティ統括（室等）	セキュアシステムプランナー	Software Development
セキュア開発管理	ノーティフィケーション	システム部門責任者	セキュアシステムデベロッパー	Systems Architecture
脆弱性診断	コマンダー、トリアージ	システム管理者	セキュアアプリケーションデベロッパー	Technology R&D
情報セキュリティアドミニストレーション	インシデントマネージャー、インシデントハンドラー	ネットワーク管理者	セキュリティマネージャー	Systems Requirements Planning
情報セキュリティアナリシス	キュレーター	CSIRT責任者	セキュリティオーディター	Test and Evaluation
CSIRTキュレーション	リサーチャー	サイバーセキュリティ事件・事故担当	システムリスクアセッサー	Systems Development
CSIRTリエゾン	ソリューションアナリスト、セルフアセスメント	セキュリティ設計担当	ペネトレーションテスター	Data Administration
CSIRTコマンド	脆弱性診断士	構築系サイバーセキュリティ担当	ネットワークリスクアセッサー	Knowledge Management
インシデントハンドリング	教育・啓発	運用系サイバーセキュリティ担当	リサーチャー	Customer Service and Technical Support
デジタルフォレンジクス	フォレンジックエンジニア	CSIRT担当	フォレンジックエンジニア	Network Services
情報セキュリティインベスティゲーション	インベスティゲーター	SOC担当	インテリジェンスアナリスト	Systems Administration
情報セキュリティ監査	リーガルアドバイザー	ISMS担当	インシデントレスポンダー	Systems Analysis
	IT企画部門	システム企画担当	セキュアオペレーター	Legal Advice and Advocacy
	ITシステム部門	基幹システム構築担当		Training, Education, and Awareness
	情報セキュリティ監査人	基幹システム運用担当		Cybersecurity Management
		WEBサービス担当		Strategic Planning and Policy
		業務アプリケーション担当		Executive Cyber Leadership
		インフラ担当		Program/Project Management
		サーバ担当		Cyber Defense Analysis
		DB担当		Cyber Defense Infrastructure Support
		ネットワーク担当		Incident Responder
		サポート・教育担当		Vulnerability Assessment and Management
		ヘルプデスク担当		Threat Analysis
		監査責任者		Exploitation Analysis
		監査担当		All-Source Analysis
		特定個人情報取扱責任者		Targets
		特定個人情報取扱担当		Language Analysis
		個人情報取扱責任者		Collection Operations
		個人情報取扱担当		Cyber Operational Planning
				Cyber Operations
				Cyber Investigation
				Digital Forensics

（論点２：専門人材）登録セキスペにおける代表的な人材タイプ（登録セキスペ実態調査より）

- 登録セキスペ実態調査※において、担当業務の相関分析から、ユーザ・ベンダーともに代表的な人材タイプは①セキュリティマネジメント系、②セキュア開発系、③セキュリティ運用系　であることが見えてきている。

担当業務の相関分析（精査中）

主業務以外で担当している業務

コーポレートITの企画・構築・管理等に関わっている登録セキスペ（2,208名）の回答内容

主業務として選択した人数	他に担当しているサイバーセキュリティ関連業務（責任者、主導的な実務者、補佐的な実務者全て含む）												
	①サイバーセキュリティに関する経営判断	②サイバーセキュリティ管理体制の構築	③サイバーセキュリティ管理体制のマネジメント	④セキュア設計・開発・構築・評価	⑤ITシステム・サービスのセキュリティ面での運用・管理	⑥サイバーセキュリティ対策機器の運用・保守	⑦監視・情報収集	⑧脆弱性診断、情報セキュリティ監査	⑨インシデント対応	⑩セキュリティ技術やサイバーセキュリティ対策に関する調査・研究	⑪サイバーセキュリティに関する教育・人材育成	⑫その他の業務	平均担当業務数
①サイバーセキュリティに関する経営判断	46	38	36	24	30	31	31	27	36	33	21	1	7.8
	2.1	82.6	78.3	52.2	65.2	67.4	67.4	58.7	78.3	71.7	54.3	2.2	
②サイバーセキュリティ管理体制の構築	130	91	119	102	110	98	103	99	109	105	102	3	9.0
	5.9	70.0	91.5	78.5	84.6	75.4	79.2	76.2	83.8	80.8	78.5	2.3	
③サイバーセキュリティ管理体制のマネジメント	156	98	144		115	134	116	127	126	142	124	127	3	9.1
	7.1	62.8	92.3		73.7	85.9	74.4	81.4	80.8	91.0	79.5	81.4	1.9	
④セキュア設計・開発・構築・評価	468	72	120	123		339	239	211	205	244	206	139	1	5.1
	21.2	15.4	25.6	26.3		72.4	51.1	45.1	43.8	52.1	44.0	29.7	0.2	
⑤ITシステム・サービスのセキュリティ面での運用・管理	641	184	297	303	401		434	425	341	480	337	283	3	6.4
	29.0	28.7	46.3	47.3	62.6		67.7	66.3	53.2	74.9	52.6	44.1	0.5	
⑥サイバーセキュリティ対策機器の運用・保守	233	62	110	100	123	188		187	125	189	132	105		6.7
	10.6	26.6	47.2	42.9	52.8	80.7		80.3	53.6	81.1	56.7	45.1	0.0	
⑦監視・情報収集	102	27	45	43	64	71	67		56	77	64	39	1	6.3
	4.6	26.5	44.1	42.2	62.7	69.6	65.7		54.9	75.5	62.7	38.2	1.0	
⑧脆弱性診断、情報セキュリティ監査	97	22	41	40	54	56	37	47		54	56	48	2	5.6
	4.4	22.7	42.3	41.2	55.7	57.7	38.1	48.5		55.7	51.5	49.5	2.1	
⑨インシデント対応	184	34	83	82	82	118	92	108	77		101	84	1	5.7
	8.3	18.5	45.1	44.6	44.6	64.1	50.0	58.7	41.8		55.4	45.7	0.5	
⑩セキュリティ技術やサイバーセキュリティ対策に関する調査・研究	72	14	24	22	31	32	23	32	20	23		34		4.5
	3.3	19.4	33.3	30.6	43.1	44.4	31.9	44.4	27.8	31.9		47.2	0.0	
⑪サイバーセキュリティに関する教育・人材育成	42	24	28	32	29	36	33	32	22	36	39		1	6.0
	2.8	57.9	45.2	51.6	46.8	58.1	53.2	51.6	35.5	58.1	62.9		1.6	
⑫その他の業務	17	6	7	7	6	10	5	7	7	7	7	9		5.6
	0.8	35.3	41.2	41.2	35.3	58.8	29.4	41.2	41.2	41.2	41.2	52.9		
合計	2,208													

担当業務のまとまり①：セキュリティマネジメント系

担当業務のまとまり③：セキュリティ運用系

担当業務のまとまり②：セキュア開発系

主として担当している業務

上段：人数
下段：%（主業務ごと）

:70%以上
:50%～70%未満
:30%～50%未満
:10%～30%未満
:10%未満

人材タイプ（数値精査中）

自組織のIT担当（主にユーザー企業）	顧客のIT業務を請け負う（ベンダー企業）
①セキュリティマネジメント系 ・全体の**5%**程度 ・幅広く業務を担当	**①セキュリティマネジメント系** ・全体の**3%**程度 ・幅広く業務を担当
②セキュア開発系 ・全体の**9%**程度 ・運用管理を併せて担当する人が多い	**②セキュア開発系** ・全体の**18%**程度 ・運用管理を併せて担当する人が多い
③セキュリティ運用系 ・全体の**21%**程度 ・運用関連業務をまとめて担当する人が多い	**③セキュリティ運用系** ・全体の**20%**程度 ・運用関連業務をまとめて担当する人が多い
調査・研究 ・全体の2%程度	脆弱性診断・監査 ・全体の2%程度
人材育成 ・全体の1%程度	調査・研究 ・全体の2%程度
	人材育成 ・全体の1%程度

※平成30年度、IPAにて登録セキスペ約1万7千人を対象に実態調査アンケートを実施。7,537件の回答を得た。本調査結果は現在分析中で、別途IPAより公開する予定。

（論点２：専門人材）登録セキスペ実態調査結果やこれまでの議論を踏まえた考察①

- 専門性が高い分野における主要な役割は、例えば以下のように大括り化できる可能性がある。

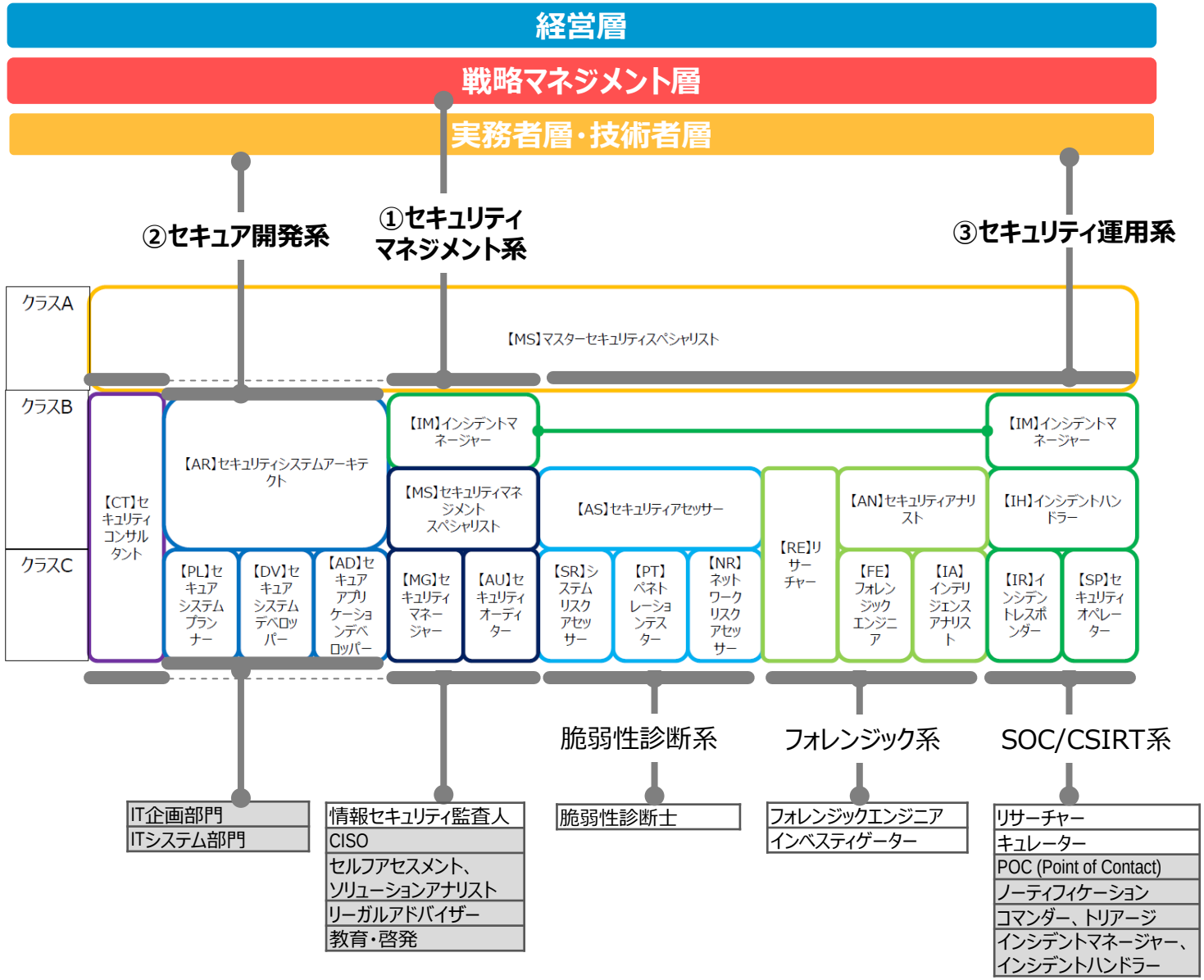
ユーザー企業

ITベンダー

NEC・日立・富士通「統合セキュリティ人材モデル」（14の役割）

セキュリティベンダー

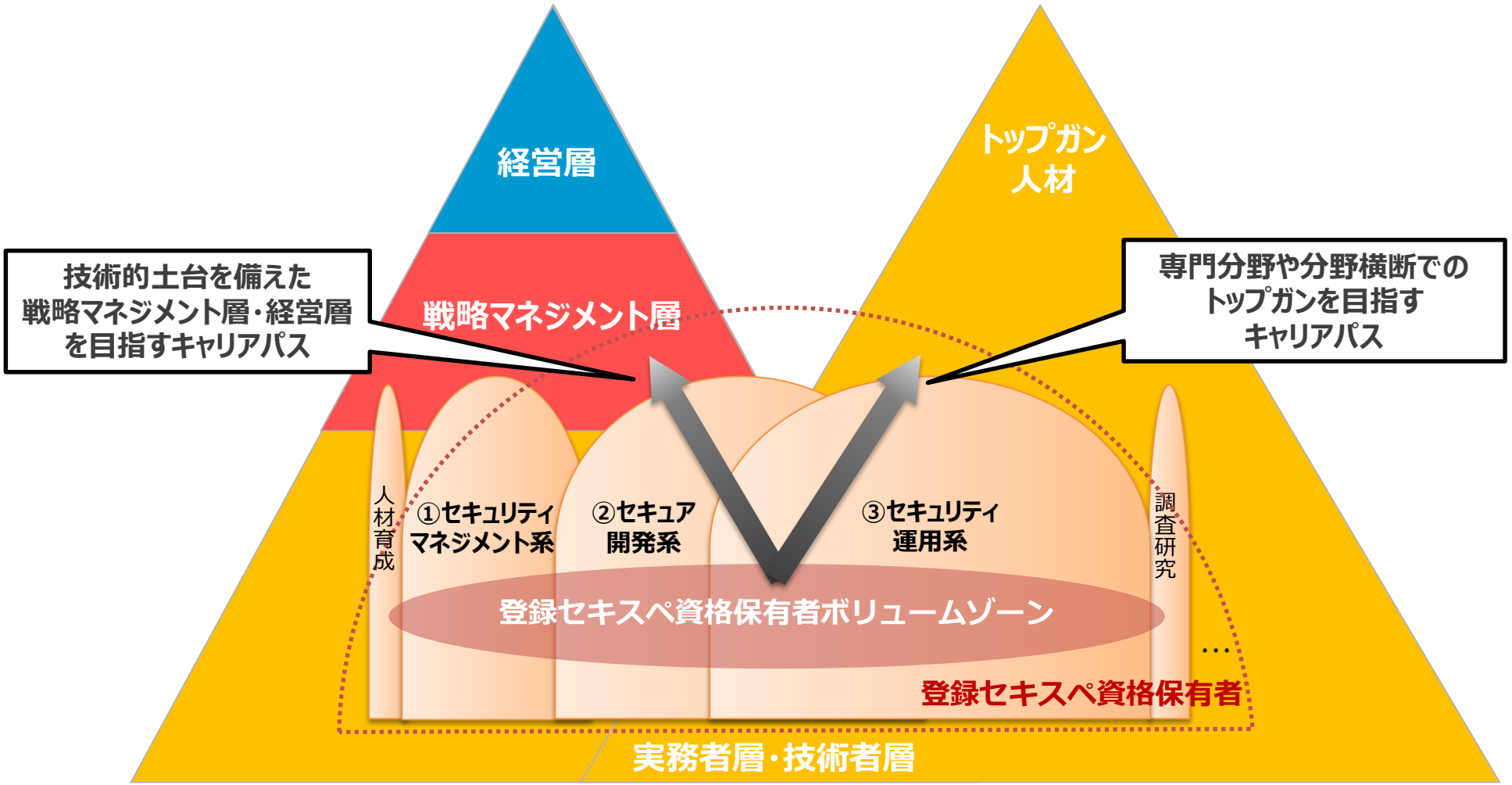
日本ネットワークセキュリティ協会（JNSA）「SecBok 2019」（16の役割）



※ ▭ は主にユーザ企業の役割

（論点２：専門人材）登録セキスペ実態調査やこれまでの議論を踏まえた考察②

- キャリアパスとしては大きく分けて、①技術的土台を備えた戦略マネジメント層・経営層を目指すキャリアパス、②トップガン人材を目指すキャリアパス、が存在すると考えられる。
- 登録セキスペ資格は、様々なセキュリティ上の役割における体系的・共通的なセキュリティ知識・スキルを身につけることに有効であることが見えてきた。



（論点２：専門人材）登録セキスペ & ITSS+の更なる改善

- 情報処理安全確保支援士（登録セキスペ）制度は、平成29年4月に登録を開始し、平成30年10月現在での登録者数は17,360人となったところ。
- 登録開始からまもなく３年目となり、ある程度の運用実績も積み上がってきたところ、調査結果も踏まえ、ＩＴＳＳ＋（セキュリティ領域）や登録セキスペ制度の運用について更なる改善を検討する。

【現行のITSS+（セキュリティ領域）】

領域	セキュリティ領域												
専門分野	情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTキュレーション	CSIRTリエゾン	CSIRTコマンド	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査
レベル7													
レベル6													
レベル5													
レベル4													
レベル3													
レベル2													
レベル1													
登録ｾｷｽﾍﾟ想定業務	経営課題	設計・開発		運用・保守				緊急対応					監査

領域	セキュリティ領域
専門分野	
レベル7	更なる改善を検討
レベル6	
レベル5	
レベル4	
レベル3	
レベル2	
レベル1	

※ITSS＋（セキュリティ領域）は、セキュリティ業務の役割の観点により、経営課題への対応から設計・開発、運用・保守、セキュリティ監査における13の専門分野を具体化。**登録セキスペが想定する業務を包含。**

（１）『セキュリティ人材活用モデル』の構築

（２）戦略マネジメント層の育成

（３）産学官の連携強化

本年度の戦略マネジメント層育成事業の結果概要

- IPA産業サイバーセキュリティセンターにおいて実施した「戦略マネジメント系セミナー」は、本年度初めて実施したものであったが、１７名が参加し、業種や立場の異なる参加者の間で活発な議論が行われた。
- 一橋ビジネススクールICSの協力で行われた、カリキュラムにサイバーセキュリティを組み込んだ「デジタル・トランスフォーメーション時代における経営人材育成プログラム」は、官民合わせて３０社が参加し、知識の習得とともに、情報の共有が行われた。

産業サイバーセキュリティセンター「戦略マネジメント系セミナー」

- 平成30年11月～12月（全７回）
- １７名（うち６名は部長以上）が参加
- 前半は専門家からの講義、後半はケース討議（グループディスカッション）の２部構成で実施
- アンケート調査の結果、参加者の約９割が有意義であったと回答


一橋ビジネススクールICS協力「デジタル・トランスフォーメーション時代における人材育成プログラム」

- 平成30年9月～１１月（全12日間※修了式除く）
- 官民合わせて30社が参加
- DXに関するリテラシーが向上し、参加者間でのネットワークが構築


産業サイバーセキュリティセンターにおける「戦略マネジメント系セミナー」については、本年度の実施結果を踏まえたカリキュラムや実施期間を見直しを行い、来年度も実施する方向で検討中

（１）『セキュリティ人材活用モデル』の構築

（２）戦略マネジメント層の育成

（３）産学官の連携強化

国立高専機構と産・官との連携促進・具体化に向けて

- 国立高専におけるセキュリティ教育が産業界の求める人材像とも整合していくためには、産学官の継続的な協力関係が必要。
- このため、国立高専機構がIPAや業界団体（CRIC CSF、JNSA）との協力内容を具体化していくための議論を継続的に実施。

＜高専・産・官の対話の場（イメージ）＞

継続的な協力体制

学　高専機構　等
- ■高度セキュリティ人材、情報系人材、非情報系人材
- ■教員　等

産　企業・業界団体
- ■CRIC CSF、JUAS、JNSA
- ■ユーザー企業、IT・セキュリティベンダー　等

ニーズ・シーズの整理・具体化 ▶ 協力の検討 ▶ 産業界に求められるセキュリティ人材の育成・輩出

- ・トップガンの育成支援
- ・キャリア教育
- ・機械・建築・生物等の分野別教材の開発・素材提供
- ・セキュリティ教員向けのFD（Faculty Development）
- ・講師派遣
- ・産業界に求められるセキュリティ人材像の共有
- ・適切なプレイヤーとのマッチング

官　関係省庁・独法等
- ■NISC、文科省
- ■IPA、JPCERT/CC　等

国立高専機構と産・官との連携促進・具体化の状況

- METI、国立高専機構、IPA及び業界団体（CRIC CSF、JNSA）において具体的連携について検討中。

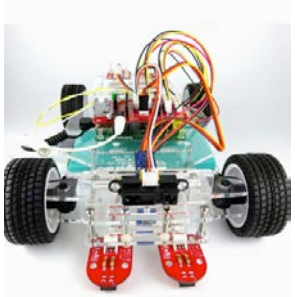
使用できるインフラ
- 演習設備
- 同時中継
  (全国高専間で配信可)
- 仮想空間

国立高専卒業生 約1万人/年の内訳（セキュリティスキルレベル）	コンテンツ開発・授業の提供 (PowerPoint、ビデオ等)	セキュリティ合宿に関する協力
	パターン①：90分程度 ・高専教員がコンテンツを使って講義 又は 企業等の方が講義 （拠点校から全国各校に同時配信も可） **パターン②：15分程度** 授業冒頭や隙間時間でビデオ放映	**高度セキュリティ合宿**（1泊2日） 年2回ペースで開催（NWトラブル演習等）参加者：35名程度 **KOSENセキュリティコンテスト**（1泊2日） 年1回ペースで開催（CTF）参加者：130名程度 ※開催期間中の一部の時間を利用して、一線で活躍するホワイトハッカーから講義を実施可能。
約1% トップガンの学生 → 主に**セキュリティ企業**に就職	※トップガンの学生は、全国各校、各学科に散らばっているため、通常の授業時間で集合する機会がない。	• **JNSAが講師の派遣を検討中。** • **METIがセキュリティ専門官の派遣を検討中。**
約20% 情報系学科の学生 → 主に**IT企業**に就職	• **IPAが地元のICSCoE終了生による講義を検討中。** • **JNSAがコンテンツ開発を検討中。**	• **JNSAとSECCONビギナーズに係る協力を検討中。**
約80% 非情報系学科の学生 → 主に**ユーザー企業**に就職	• **CRIC CSFが業界別（例．機械、電気、建築等）のコンテンツ開発や授業提供について検討中。**	※セキュリティ合宿のような機会は特段なし。
KOSEN 国立高等専門学校機構 国立高専教員	※授業実施側のため。	• **JPCERT/CCが情報担当教員向け研修に講師を派遣。** • **IPAがセキュリティキャンプ全国大会の見学について検討中。** • **教師向け合宿において、METIによるセキュリティ専門官の派遣や、IPAによるAppGoatの使用方法等の派遣講義を検討中。**

（参考）国立高専が所有する設備の例

1．演習設備

- 2016年、地域の情報セキュリティ教育の拠点とするため、拠点校に**セキュリティ演習環境を整備**。2017年には拠点を増やし、10箇所にした。
- 2018年度末までに、石川高専、佐世保高専、高知高専に、**IoT演習とSOC演習設備を整備**。情報系を含め、全学科の学生を教育対象とする。
- 主な設備は、SOC設備、IoTスマートハウス、IoTカー（Docomo FaBo）、エレベーター模擬システム。

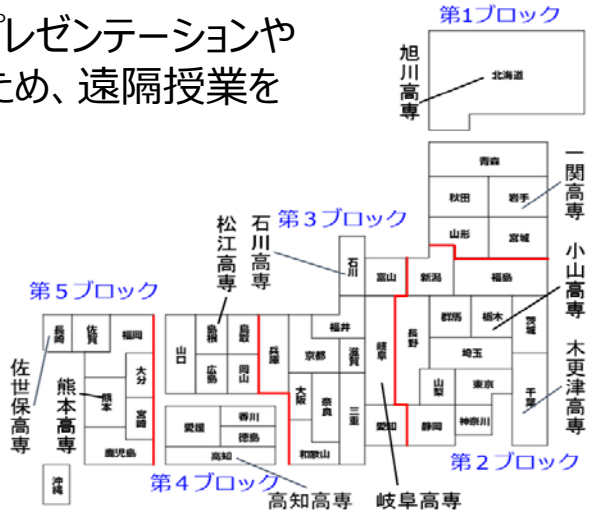


FaBoロボットカー

2．コンテンツ配信設備

- 全国の国立高専に、統一ネットワークシステムとしてBlue Jeans Networkを導入済み
- 講義等を**全国51高専間でネット配信可能**
- ビデオ映像や音声を配信でき、プレゼンテーションやデスクトップの共有が可能であるため、遠隔授業を実施することも可能。

（日立製作所出前授業は希望する高専に遠隔配信）



1．経営

2．人材

3．地域

4．国際

（参考）地域の実態
～大阪商工会議所における調査

- 大阪商工会議所、東京海上日動は神戸大学の協力のもと、国内で初めて、中小企業に対するサイバー攻撃の実態を把握するための実証事業を実施。
- 調査の結果、中小企業においてもサイバー攻撃を受けている恐れがあることがわかった。

調査内容

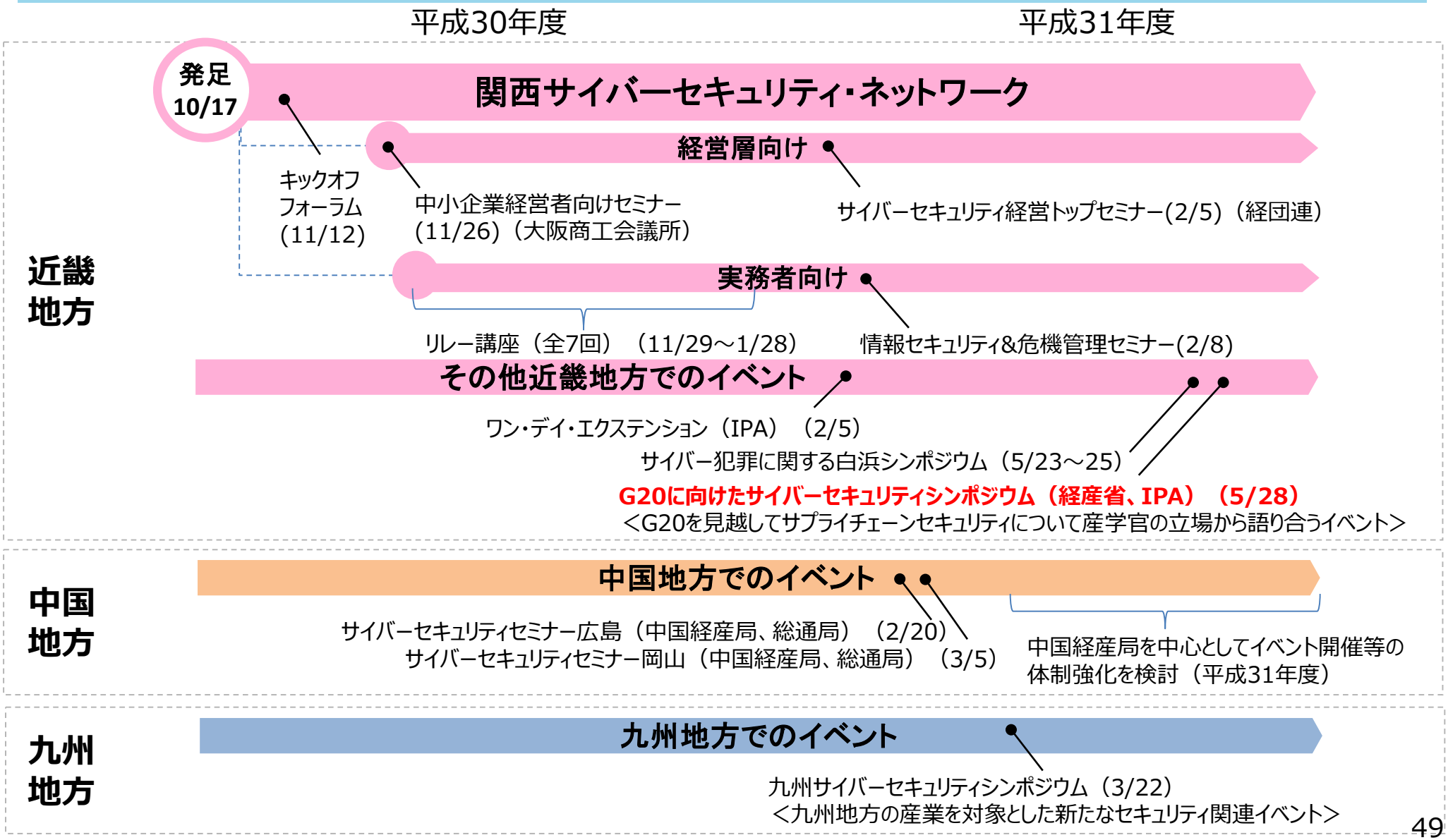
- 実証期間：平成30年9月～平成31年1月
- 実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間にわたり収集し、サイバー攻撃に関する調査、分析を行う。

調査結果（中間報告）

- 調査した30社全てでサイバー攻撃を受けていたことを示す不審な通信が記録されていた。
- 少なくとも5社ではコンピューターウイルスに感染するなどして、情報が外部に流出したおそれがあることが分かった。
- 今後さらに調査を進め、最終的な調査結果を今年４月頃に公表する。

地域における取組の現状

- 関西サイバーセキュリティ・ネットワークをはじめとし、地域大での取組が進みつつある。



産業サイバーセキュリティセンターにおける地域への取組状況

- IPAに設置された産業サイバーセキュリティセンター（ICSCoE）においても、これまで東京でのみ行ってきたプログラムを大阪で初めて開催。
- また、中核人材育成プログラムの修了生は、継続的にコミュニティを維持しながら全国に存在するところ、中京圏の修了生・派遣元企業の協力を得て、名古屋で説明会を実施。
- 来年度以降も引き続き、地域への取組を進めていく予定。

地方でのプログラムや説明会の実施

- ２月５日、ICSCoEのワン・デイ・エクステンションを大阪で実施。大阪を中心に関西の企業から多数の参加（４５名）があった。
- ３月１３日、中部でも、ICSCoE修了生と派遣企業が講師となるセミナー。２２名が参加。地域の情報ハブとして活躍。

＜ICSCoE修了生による講演＞

IN 大阪

IN 中部①

IN 中部②

引き続き、地方でのプログラムの実施や説明会の開催を検討

高専機構と連携し、高専の学生や教員を対象に、出前授業や合宿へ産業サイバーセキュリティセンターの講師や修了生の派遣を検討

2018年度 → **2019年度**

地域における課題と対応する取組の整理

- 徐々に取組が充実してきているものの、まだまだ地域では不足感が存在。
- 特に具体の対策を検討・推進する上で、地域では下記の課題が顕著
  ①セキュリティを担う実務担当者に信頼できる相談相手・コミュニティが少ない。
  ②一般的なセミナーは多少増えてきていても、大企業向けであったりセキュリティベンダー目線であったりで、地域の企業が自社に落とし込む上での難易度がある。

ターゲット企業	課題	取組（赤字は地域で不足感のある施策）
セキュリティを全く気にしていない企業	サイバー攻撃のターゲットになり得るという認識がない	中小企業のサイバー攻撃に関する実態調査（お助け隊等） 中小企業の情報セキュリティ対策ガイドライン等を通じた普及啓発
セキュリティに取り組もうとしている企業	社内に相談相手がいない（ひとり情シス状態）	**地域における人脈形成支援**
	セミナーが少なく、学ぶ機会がない	講習能力養成セミナー等のイベント（IPA）
	セキュリティベンダーが少なく、相談相手がいない	**自社の具体的な対策への落とし込み促進**
	必要性がわかっても何をやればいいかわからない	経営プラクティス集（IPA）
	大企業向けのソリューションが多く、中小には使いにくい	**自社の具体的な対策への落とし込み促進**
	どのセキュリティソリューションを選択すべきかの判断ができない	適正な市場環境の整備（情報セキュリティサービス審査登録制度）
ベンダー企業等	ニーズが明確化されていないため、セキュリティがビジネスになりにくい	中小向けサービスの創出支援（お助け隊等）
	学生がセキュリティを学んでも就職先が少なく、人材が首都圏に流れる（地元で人材が育たない）	**自社の具体的な対策への落とし込み促進**

①地域における人脈形成支援

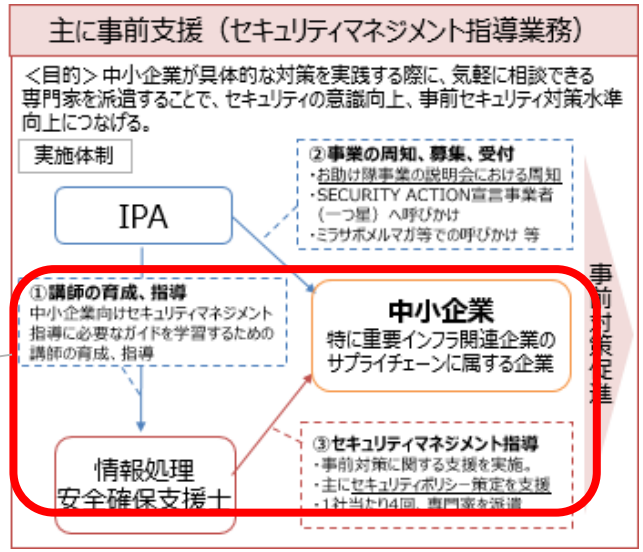
- 単に「知る機会」が少ないということとともに、「相談相手が不足」していることから十分な対策が取れているかについて、地域の企業担当者の不安感は強いのではないか。
- 地域内で企業をまたいだセキュリティ担当者同士の人脈を形成することは、担当者のモチベーション維持、社会全体としてセキュリティレベルを向上させるために重要である。

地方版コラボレーション・プラットフォームの開催

②自社の具体的な対策への落とし込み促進

- 専門家（登録セキスペ）による中小企業支援を強化することで、実践的な対策を促すとともに、専門家自身の地域での活躍を促進する。
- また、中小企業でも使いやすいセキュリティ対策の普及・創出を促すため、NIST SP800-171等のガイドラインに準拠する上で有効な製品・サービスを調査・検証する。

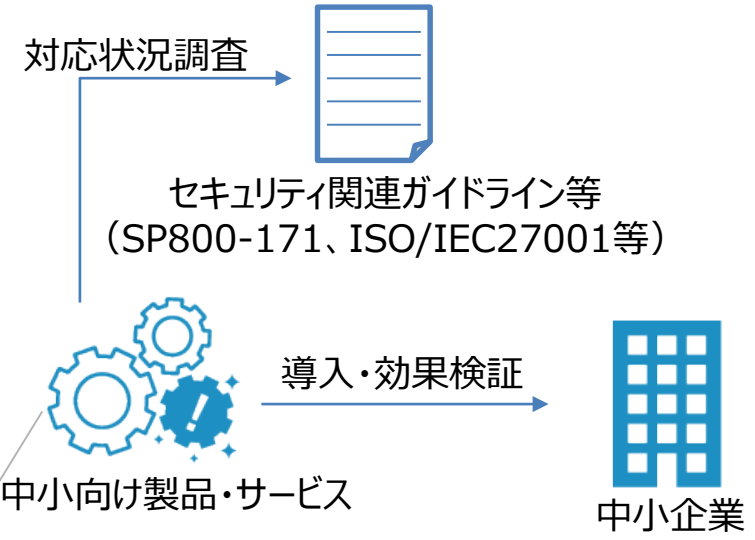
＜登録セキスペ支援事業＞



- 対策に困っている中小企業に対して登録セキスペを派遣し、実践的な対策を支援。
- 地域の登録セキスペが地元企業の支援を行い、地元での活躍の機会を増やすことで、地域のセキュリティ産業を活性化。

＜中小企業向け製品の検証事業＞

平成30年度第2次補正予算
中小企業等強靭化対策事業にて実施



中小向け製品・サービスの例
- 導入が容易であること
- 運用に専門性が不要であること
- コストが安価であること

1．経営

2．人材

3．地域

4．国際

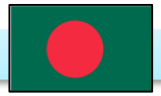
ASEAN等へのセキュアな電力制御システム（SCADA※）の導入に向けた取組

※SCADA : Supervisory Control And Data Acquisition

- 今年度、ASEAN等においてセキュアな電力制御システムに関する研修事業等を実施。

対象国・地域の広がり


ベトナム


バングラデシュ


カンボジア


ラオス


ミャンマー

ビジネス化に向けた取組の深化

相手国の理解醸成

「平成29年度　ベトナムにおける電力制御システムに関するセキュリティ規制策定能力向上支援事業」

ベトナムにおいて、電力分野のサイバーセキュリティ能力の向上のための専門家派遣と訪日研修を一財・海外産業人材育成協会（AOTS）において実施。

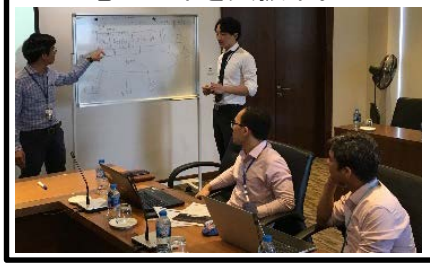
「平成30年度　技術協力活用型・新興国市場開拓事業（インフラ海外展開支援）事業」

カンボジア、ラオス、ミャンマーにおいて、サイバー攻撃に強い電力制御システム（SCADA）の導入のため、現地の電力企業向けに研修を実施中。

企画・計画支援

「平成30年度　質の高いｲﾝﾌﾗの海外展開に向けた事業実施可能性調査事業」

ベトナム、バングラデシュにおいて、サイバー攻撃に強い電力制御システム（SCADA）の導入のため、企画・計画段階から現地の電力企業を支援中。



写真：TEPCO IEC(株)

マルチ・バイを通じた国際協調への取り組み

- **「サイバー・フィジカル・セキュリティ対策フレームワーク」**を軸に、各国のステークホルダーと議論、マルチの会議で紹介し、サイバー・フィジカル・セキュリティに関する共通の認識を醸成。

- **VDE Tech Summit　（2018年11月@ドイツ・ベルリン）**
  - VDE（ドイツ電気技術者連合）主催の国際会議においてサイバー・フィジカル・セキュリティ対策フレームワーク（以下「フレームワーク」）を紹介。
- **日イスラエル電力セキュリティWS（2018年11月@東京）**
  - イスラエル電力公社(IEC)から日本の電力事業者に対し、電力分野での取組を紹介し、意見交換。
- **Cybertech Tokyo 2018（2018年11月@東京）**
  - イスラエル主催の国際展示会/シンポジウムにおいて、瀧波政務官が基調講演。西山商務情報政策局長等から当省の取組及び「フレームワーク」について紹介。
- **OECD Global Forum（2018年12月@フランス・パリ）**
  - OECD主催フォーラムのパネルディスカッションにおいて、「フレームワーク」を紹介し、意見交換。
- **サイバーイニシアティブ東京2018（2018年12月@東京）**
  - 日経BP主催の国際会議において、世耕大臣が基調講演。IoTセキュリティに係るパネルディスカッションにおいて、奥家サイバーセキュリティ課長から「フレームワーク」を紹介し、議論。
- **日EU・ICT戦略WS（2018年12月@オーストリア・ウィーン）**
  - EU・総務省主催のWSにおいて、当省の取組及び「フレームワーク」について紹介。

- **CES 2019（2019年1月@米・ラスベガス）**
  - 世界最大規模の見本市において、当省の取組、「フレームワーク」を紹介。
- **日イスラエル・イノベーション・ネットワーク総会（2019年1月@イスラエル・エルサレム）**
  - 世耕大臣とコーヘン・イスラエル経済産業大臣との間で、両国のサイバーセキュリティ協力について協議。
- **ECSO-EUNITY 日欧WS（2019年1月@オーストリア・ウィーン）**
  - 欧州サイバーセキュリティ機構主催のWSで、当省の取組、「フレームワーク」について紹介。
- **日豪サイバー協議（2019年2月@オーストラリア・キャンベラ）**
  - サイバーセキュリティに係る日豪の政府間協議において、当省の取組、「フレームワーク」について紹介。
- **日印サイバー協議（2019年2月@東京）**
  - サイバーセキュリティに係る日印の政府間協議において、当省の取組、「フレームワーク」について紹介。
- **日米IED 経済協力WS（2019年3月@米・ワシントンDC）**
  - インターネットエコノミーに係る米国務省、総務省主催の協議において、当省の取組、「フレームワーク」について紹介。